Prüfbericht nach OPDV-Stellungnahme Nr. 1/2006

LORA in der Version: 2.4.2.0.7

(**Abschlussergebnis**)

Dokumentversion 3.13 vom 11.06.2013 12:18

Dieser Prüfbericht ist nur gültig, wenn er komplett weitergegeben wird, also alle Seiten vom Deckblatt bis zur Unterschriftenseite enthält.
Unvollständig weitergegebene Dokumente sind ungültig!

Die Abschnitte 4.1 und 4.2 enthalten Auflagen.





Inhaltsverzeichnis


INFORMATIKZENTRUM
DER SPARKASSEN-
ORGANISATION GMBH


INFORMATIKZENTRUM
DER SPARKASSEN-
ORGANISATION GMBH


SIZ
INFORMATIKZENTRUM
DER SPARKASSEN-
ORGANISATION GMBH



Versionsführung dieses Dokumentes:

Wer	Wann/ Version	Was
Hr. König	V130424 V3.13	▪ Berücksichtigung der Unterlagennachlieferung vom 26.3.13, siehe Literaturverzeichnis ab [149]

1 Vorwort und Zusammenfassung

Die in den letzten Jahren eingeführten Internet-basierten Infrastrukturen, wie sie bspw. die auf Browsern basierenden Client- und Serverarchitekturen erfordern, eröffnen den Anwendern die komfortable Abwicklung von Transaktionen ohne komplexe Softwareinstallation auf den Arbeitsplatzsystemen. Zugleich bringen die neuen Technologien neue Risikopotentiale mit sich, die mit immer sorgfältigerer Planung, Umsetzung und Überprüfung der IT-Anwendungen und Infrastrukturen einzugrenzen sind.

Dies sicherzustellen ist Aufgabe des jeweiligen Projektmanagements, der beteiligten Fachabteilungen sowie der Innenrevision. Mit der Stellungnahme OPDV 1/2006 liegen Regularien für die Freigabe eines Systems vor. Soweit es sich um fremd entwickelte, komplexe Systeme handelt, wird der Aufwand hierfür jedoch zunehmend größer. Wenn der Einsatz des Systems dann noch bei mehreren Betreibern vorgesehen ist, dann bietet es sich an, die Freigabe in eine Programmfreigabe und eine Einsatzfreigabe aufzuspalten.

- Im Rahmen der **Programmfreigabe** sind die fachliche Eignung entsprechend den Anforderungen des Fachkonzepts, die sachgerechte Umsetzung in der Programmierung innerhalb eines geordneten Programmentwicklungsverfahrens, der erfolgreiche Test von Verarbeitungsfunktionen und -regeln innerhalb der Anwendung (ggf. einschl. Schnittstellen) sowie das Vorliegen einer aktuellen Verfahrensdokumentation zu beurteilen.
  Unter besonderen Umständen können Umfang und Intensität der Qualitätssicherungsmaßnahmen einer Programmfreigabe reduziert werden, ggf. sogar ganz unterbleiben. Dies kann der Fall sein
  - bei Betriebssystemen und betriebssystemnaher Software
  - bei Programmen von IT-Dienstleistern, die sich dazu verpflichtet haben, ihr Programmeinsatzverfahren nach Maßgabe dieser Stellungnahme auszurichten, und gewährleisten, dass die Einhaltung dieser Verpflichtung regelmäßig geprüft wird
  - bei typischerweise nicht bankfachlicher Standard-Software (z. B. Bürosoftware), wenn die Funktionsfähigkeit aufgrund der Vertrauenswürdigkeit in die Qualität der Softwareentwicklung der Herstellerfirma unterstellt werden kann, z. B. aufgrund des hohen Verbreitungs- und Bekanntheitsgrads
  - wenn die Programmfreigabe eines vertrauenswürdigen Dritten (z. B. DSGV, SIZ, andere Sparkasse oder IT-Dienstleister als Vertreter) i. S. dieser Stellungnahme vorliegt und eine unveränderte Programmversion eingesetzt wird
  - beim Vorliegen eines qualifizierten Softwaretestats[1] von einer anerkannten Prüfungseinrichtung[2] und dem Einsatz einer unveränderten Version des Programms. Entsprechende Nachweise sind nachvollziehbar zu dokumentieren.

[1] z. B. IDW PS 880, ISO-Normen

- Gegenstand der **Einsatzfreigabe** ist die Untersuchung der organisatorischen und technischen Prozesse des Anwenders, die den Einsatz innerhalb der vorhandenen Umgebung bestimmen, sowie die Gewährleistung der Funktionsfähigkeit von Schnittstellenprozessen zu vor- und nachgelagerten Anwendungen und der Belastbarkeit im Echtbetrieb.
  Besonderer Aufmerksamkeit bedürfen die Einbindung in das Interne Kontrollsystem und die Parametrisierung des neuen Programms sowie die Ergebnisse von Integrationstests.
  Voraussetzung für die durchzuführende Beurteilung sind das Vorliegen vollständiger und aktueller Programm- und Hardwareübersichten sowie angemessene Verfahren in den Bereichen Beschaffung und Change-Management.

Im Verlauf der Prüfung kam auch die *Checkliste Prüfungen nach OPDV 1/2006* des SIZ zum Einsatz. Diese Liste baut auf der Stellungnahme Nr. 1/2006 des Fachausschusses OPDV auf und berücksichtigt die Praktiken und Erfahrungen mit DV-Projekten innerhalb der Sparkassen-Finanzgruppe. Dieses Testat ist somit eine thematisch umfassende und unabhängige Analyse des Entwicklungs-, Qualitätssicherungsprozesses sowie des Praxiseinsatzes, der dem Freigabeverfahren nach OPDV 1/2006 unterliegt. Das Testat berücksichtigt insbesondere auch Aspekte des Projektmanagements, der IT-Qualität, der Softwareentwicklung sowie der IT-Sicherheit.

1.1 Benutzung / Zweck des Dokumentes

Kursive Texte kennzeichnen Originalzitate aus anderen Dokumenten oder Vorgaben.

Formulierungen in Fettschrift außerhalb von Überschriften stellen Auflagen dar.

1.2 Prüfgegenstand

1.2.1 Identifizierung

Im Rahmen der hier dokumentierten Prüfung ist die erstellte IT-Anwendung *LORA* in der Version 2.4.2.0.7 [147] und deren Herstellungsprozess bei der on-geo GmbH[3] zu untersuchen und zu bewerten [IDW PS 880, Tz2].

Der Prüfbericht darf auch verwendet werden, um Einsatzfreigaben ähnlicher Versionen durchzuführen, dabei hat aber eine Bewertung stattzufinden, welche der Teilaussagen auch für die neuere Version verwendet werden darf.

1.2.2 Produktbeschreibung und -abgrenzung

Gegenstand der Prüfung ist ein Softwaresystem namens *LORA*. *LORA* ist Unterstützungssoftware für mit Immobilien gesicherte Kreditvergaben. *LORA* dient dabei der Beauftragung und Unterstützung des Immobiliengutachters. Die Kernfunktionalität [ISO/IEC 9126] der *LORA*-Anwendung besteht hinsichtlich Berechnung und Erstellung eines Immobiliengutachtens:

> [153, Zusammenfassung]: *LORA unterstützt als Systemlösung den kompletten Geschäftsprozess der Wertermittlung sowohl für wohnwirtschaftliche und gewerbliche Immobilien über formelle Gutachten als auch für die vereinfachte und teilautomatisierte Wertermittlung von Standardimmobilien (Eigentumswohnungen, Ein-/Zweifamilienhäuser, …) innerhalb der Kleindarlehensgrenze*.

---

[2] z. B. Prüfungsstellen, BSI, Wirtschaftsprüfungsgesellschaft , TÜV-IT

[3] Nachfolgend mit Hersteller abgekürzt.

Technisch ist *LORA* eine in VisualBasic.NET(VB.NET) implementierte Client-/Server- Anwendung. *LORA* wird auf einem Citrix-fähigen Arbeitsplatz als Client-Anwendung ausgeführt und greift dabei auf den Datenbank-Server zu.

Das Softwaresystem ist gegliedert in mehrere Komponenten. Für eine nähere Beschreibung siehe die entsprechenden Handbücher.

Die Prüfaussage dieses Prüfberichts bezieht sich auf die folgenden Systemkomponenten (Kernbestandteile) von *LORA*:

- zentrale LORA Datenbank
- LORA Client (LORA Sparkassen Edition, LORA Speed oder LORA Sales).

Die folgenden mit dem Produktumfang ebenfalls ausgelieferten oder auslieferbaren Systemkomponenten sind nicht Bestandteil der Überprüfung. Allgemeine Aussagen der vorliegenden Prüfungsdokumentation gelten daher nur dann auch für diese Systemkomponenten, wenn explizit darauf hingewiesen wird:

- Dienstleistungen von on-geo [153, Zusammenfassung] wie z. B. der Online-Zugang zu Research-Daten, Integration von Research-Daten und die Online-Beauftragung für Besichtigungen und externe Gutachten.
- Erstellung von Rechnungen oder Honorarberechnungen,
- Schnittstellentool zur Kreditsachbearbeitung und Sicherheitendatenbanken, VDP [131], VÖB, europace und vielen weiteren Systemen [153, Überblick],
sowie die Schnittstelle zu ELAXY [153, LORA Immobilienplattform],
- automatische Adressvalidierung und Georeferenzierung [109, 4.4.5.8 GEOREFERENZIERUNG],
- Application Service Providing, siehe http://www.on-geo.de/is-cms/index.php?id=85 [156]
- LORA Portfolio und die Schnittstelle zum neuen LORA Portfolio [109, 4.4.5.11 Schnittstelle zu LORA - Das neue Portfolio], andere LORA-Lösungen wie z. B.: LORAi, LORA Compact, LORA Connect und LORA Connect plus [153, Überblick],
- VÖB Analyse [109, 4.6.10.3 VÖB-Analyse].
- LORAi, Lösung mit englischer Oberfläche für ausländische Gutachter [153, Überblick],
- LORA Compact, Connect und Connect plus als Lösungen für selbständige Gutachterbüros [153, Überblick],
- LORA Portfolio für die Bewertung und Analyse von Immobilienportfolien [153, Überblick],
- ARGUS Valuation DCF Software ([153, Komponente 1: Bewertungsalgorithmen] und Testprotokolll WR 2009 der Lora-Version 2.3), siehe auch Abschnitt *1.2.2.1 Schnittstellen*,

1.2.2.1 Schnittstellen

- Benutzerschnittstelle.
Fachliche Vorgaben dieser Schnittstelle sind in der Gesamtheit der Vorversionen und mit der Gesamtheit der Kunden definiert worden, die sinnvolle Umsetzung wurde jeweils von Pilotanwendern überprüft.



- Administrationsschnittstelle (Admin-Console) sowie Schnittstellen zum Logging bzw. Tracing, die durch die entsprechenden Handbücher beschrieben sind. Nachvollziehbare Bewertungstransaktionen werden an den Daten der Datenbank gespeichert, also wer wann Änderungen vorgenommen hat. Das verfügbare Logging ist standardmäßig auf „Nur Fehler“ eingestellt, kann aber feiner justiert werden, wobei die dann zusätzlich protokollierten Daten für das Institut nicht auswertbar sind, sondern an den on-geo-Support übergeben werden müssten. Da hierbei auch Personenbezogene Daten protokolliert und weitergegeben werden, muss durch das Vertragsmanagement des Institutes sichergestellt werden, dass entsprechende Supportvereinbarungen auch das Thema Datenschutz abdecken. Insgesamt muss seitens SIZ aber darauf hingewiesen werden, dass hier zwar Personenbezogene Daten betroffen sind, hiervon aber nur bedingt der private Bereich der Personen tangiert wird. Die meisten der im Rahmen einer Baumaßnahme oder Immobilie angesprochenen Personendaten, wie Eigentümer, Ausführende etc. sind auch in anderen teilweise öffentlichen Informationsquellen wie Kataster etc. verfügbar.
- Zentrale Datenbank
  Die Geschäftsdaten werden in einer zentralen Datenbank abgelegt, deren sicherer Betrieb im Dokument „Sicherheitshinweise - LORA Sparkassen Edition“ [152, 2.1.4 Zugriffsschutz für Datenbank und Online-Dienste] beschrieben ist.
- Lokale Datenbank
  Jeweils zu bearbeitende Gutachten werden in einer lokalen Access-Datenbank gehalten, auch deren Betrieb ist im Dokument „Sicherheitshinweise - LORA Sparkassen Edition“ beschrieben, es macht aber darauf aufmerksam, dass auf die lokale Datenbank Schreibzugriff gewährt werden muss [152, 2.1.2 Bestandteile der Software].
- Schnittstellen zur Argus-Software
  Komponenten der Argus-Software selber werden durch den Prüfbericht nicht abgedeckt, die Schnittstellen zwischen Argus und Lora düfen aber als im Prüfbericht eingeschlossen betrachtet werden.
- Krebis und Schnittstelle zu on-geo-Research-Daten
  diese beiden Schnittstellen und deren Verwendung sind nicht durch den vorliegenden Prüfbericht abgedeckt.
- Schnittstelle zum Gutachter
  Beauftragte Gutachten werden von einem ggf. externen Gutachter erstellt und mit diesem dazu ausgetauscht. Technisch geschieht dieser Austausch über verschlüsselte E-Mails.

1.3 Prüfkriterien

Die Prüfung erfolgt auf der Grundlage der von:

- Fachausschuss Ordnungsmäßigkeit und Prüfung der Datenverarbeitung, Stellungnahme Nr. 1/2006, Anforderungen an einen ordnungsgemäßen Software-Einsatz in ihrer aktuellen Fassung.

Die Prüfung erfolgte unter Hinzuziehen der folgenden Checkliste:

- Checkliste - Prüfungen nach OPDV 1/2006, Version vom 22.02.2013, SIZ



1.4 Ziel der Prüfung

Vor Inbetriebnahme eines IT-Systems innerhalb der Sparkassen-Finanzgruppe ist eine Programmfreigabe nach OPDV 1/2006 erforderlich. In diese Freigabeerklärung fließen die Ergebnisse aller am Abnahmeprozess Beteiligten ein. Als Vorbereitung auf die Freigabe analysiert und bewertet vorliegender, von einem unabhängigen Mitarbeiter des SIZ erstellte Prüfbericht den Verlauf und die jeweiligen Arbeitsergebnisse der Herstellung durch on-geo GmbH.

Das Ziel der Prüfung ist die Bewertung, inwieweit die Anforderungen der OPDV 1/2006 eingehalten sind, d. h. es wird im Prüfbericht eine Aussage zur Ordnungsmäßigkeit der Verarbeitung des IT-Systems getroffen. Sofern alle Anforderungen eingehalten sind, wird eine Empfehlung zur Freigabe ausgesprochen.

Als Besonderheit bezieht sich das konkrete Freigabeverfahren des SIZ für *LORA* lediglich auf eine „Programmfreigabe“. Vor einem tatsächlichen Einsatz von *LORA* innerhalb der Sparkassen-Finanzgruppe ist zusätzlich ein betreiberspezifisches Einsatzfreigabeverfahren zu durchlaufen. Dies muss den örtlichen Gegebenheiten des Betreibers Rechnung tragen und den Integrationsprozess berücksichtigen. Insbesondere sind seine infrastrukturellen, organisations- und bundeslandspezifischen Vorschriften und Regelungen bzw. Gesetze einzubeziehen.

1.5 Voraussetzungen der Prüfung

Für den vorliegenden Prüfbericht ist Folgendes vorausgesetzt:

- Prüfer erfüllen die persönlichen, fachlichen und formalen Voraussetzungen für die Durchführung der Prüfung nach OPDV 1/2006.
- Das IT-System bzw. IT-Produkt unterliegt den Regelungen der OPDV 1/2006.
- Grundsätzlich haben die Betreiber wie auch der Prüfer das Vertrauen in den Hersteller, dass er seine Kompetenzen nach bestem Wissen und Gewissen einsetzt. Damit mögliche Fehler vermieden oder zumindest erkannt und beseitigt werden können, gewährte der Hersteller dem Prüfer einen umfassenden und detaillierten Einblick in seine internen Abläufe. Dies beinhaltet seine Prozesse, Verfahren, Methoden und Dokumente. Hierdurch wird das Vertrauen in die Produkte des Herstellers gestärkt. Die Offenlegung dieser betriebsinternen Informationen erfolgt im wechselseitigen Vertrauen auf die Einhaltung üblicher Vertraulichkeitsregelungen. In den Prüfbericht fließen ausschließlich Informationen, die für die Analyse und Bewertung nach OPDV 1/2006 erforderlich sind.

1.6 Prüfgrundsätze und -vorgehen

Die für die Prüfung nach OPDV 1/2006 angewendeten Grundsätze sind:

- Die Prüfung begleitet den Lebenszyklus des IT-Systems bzw. IT-Produkts beginnend mit der Anforderungsdefinition bis hin zur Auslieferung an den Kunden.
- Die Prüfung bewertet sämtliche Qualitätsprozesse und schließt die fachkundige Bewertung der IT-technischen, infrastrukturtechnischen, organisatorischen, prozessualen und sicherheitstechnischen Maßnahmen ein.
- Die Prüfung bewertet auch, ob beim Softwareentwickler die Anforderungen gemäß OPDV 1/2006 eingehalten wurden.
- Die Prüfung stützt sich sowohl auf die Herstellerdokumentation und ein am [muss im Rahmen eines Testierungsprozesses noch beschrieben werden] durchgeführtes Audit beim Softwarehersteller.



- Die Prüfung wendet das „Prinzip des Unabhängigen Dritten“ an, d. h. die Abnahme wird von unabhängigen SIZ-Mitarbeitern überprüft. Die Aussagekraft der Überprüfung und die dadurch erzielbare Qualität wird so deutlich gesteigert. Das Arbeitsergebnis der unabhängigen Analyse ist vorliegender Prüfbericht.
- Die Prüfung wird unter der „going concern“ Annahme des Softwareherstellers durchgeführt, d. h. die Bewertungen werden unter der Voraussetzung getroffen, dass das die IT-Anwendung herstellende Unternehmen fortbesteht.

1.7 Grenzen des Dokuments

Dieser Prüfbericht ist thematisch sehr umfassend angelegt, so dass erwartet werden kann, dass alle IT-technischen Aspekte der Programmfreigabe nach OPDV 1/2006 abgedeckt sind. Seine Grenzen werden hier konkretisiert.

- Dieser Prüfbericht betrachtet ausschließlich die in direktem Zusammenhang mit der Informationstechnologie stehenden Aspekte, die zur erfolgreichen Projektabwicklung bzw. System- und Produktentwicklung gehören. Dies schließt sämtliche zugehörigen organisatorischen wie technischen Themen ein. Bspw. gehört das Projektmanagement ebenso zu den Aspekten wie Dokumentation, Entwicklung, Herstellertests, Abnahmetests sowie IT-Qualität und IT-Sicherheit. Nur bedingt betrachtet werden dedizierte juristische oder betriebswirtschaftliche Aspekte. Auch sind Aspekte wie die Analyse des Kundenbedarfs an anderer Stelle zu betrachten.
- Die Überprüfung erfolgt immer gegen die Produktspezifikation, deren inhaltliche Korrektheit und Vollständigkeit ausschließlich in der Verantwortung des Herstellers liegt. Die Spezifikation wird lediglich darauf hin überprüft, ob sie ausreichend vollständig und in sich schlüssig ist.
- Anforderungsdefinitionen bzw. zu Grunde gelegte Standards werden grundsätzlich nicht hinterfragt, es sei denn, dass sie offensichtlich unvollständig oder unangemessen sind.
- Insbesondere nicht enthalten ist eine Detailanalyse des IT-Systems bzw. Produkts bspw. im Rahmen eines Codereview [IDW PS 880, Tz22]. Solche tiefgehenden Analysen erforderten das Anwenden bspw. von IT-Sicherheitskriterien wie den „Common Criteria“ (ISO 15408) oder des Sicheren IT-Betriebs des SIZ, was inhaltlich sowie im Umfang ausdrücklich außerhalb dieser Prüfung liegt.
- Der vorliegende Prüfbericht greift der Einsatzfreigabe nach OPDV 1/2006 durch die zuständige Revision nicht vor. Diese Freigabe bleibt exklusiv dem jeweiligen Institut vorbehalten.
- Grundsätzlich muss jeder Betreiber vor Einsatz des Produktes sein eigenes Freigabeverfahren durchführen, welches die konkreten Gegebenheiten des Betreibers berücksichtigt. Dabei ist es empfohlen und gewollt, die aus der Programmfreigabe gewonnenen Erkenntnisse in die eigene Analyse einzubinden.
- Hinsichtlich der in [IDW PS 880, Tz19] geforderten eigenen Testfälle des Prüfers wird im Rahmen der hier dokumentierten Prüfung überprüft, ob in den vorgelegten Testprotokollen auch die Prüffälle enthalten sind, die aus Sicht des Prüfers durchgeführt werden müssten. Hierzu werden sowohl Prüfungen auf in der Software erwartete Eigenschaften als auch Prüfungen auf nicht in der Software zugelassene Eigenschaften (siehe [IDW PS 880, Tz20]) herangezogen und dabei alle potentiellen Störquellen betrachtet. Einem vorgelegten Testprotokoll wird dabei nicht blind vertraut, es wird seitens des Prüfenden hier immer ein Nachweis über die Korrektheit des Testprotokolls verlangt.



1.8 Projektbeteiligte

Hersteller und Lieferant

Hersteller und Lieferant von *LORA* ist die on-geo GmbH. Die Entwicklung hat stattgefunden in Erfurt, Gerichtsstand ist München [106, 11.6].

Betreiber

Hinweis: Die erforderliche Betreiberfreigabe seitens der Rechenzentren ist nicht Gegenstand dieses Berichts.

Abnahmen

Die on-geo GmbH ist Eigentümer von *LORA* [106, 11.7]. Eine Marktfreigabe des Herstellers für die Software liegt vor [158].

Seitens der FI liegt mit Rundschreiben Nr. 206/2009 die Information über einen bestehenden Rahmenvertrag mit dem Hersteller vor, der Sparkassen einen speziellen Lizenzierungs- oder Nutzungspreis anbietet. Weiterhin ist für LORA im „*PARSYS-Handbuch Basisadministration, Ausgabe 9, Ausgabedatum: 5/2009*“ im Abschnitt „*C 2.7.19 [-->] Berechtigungen für Fremd-Anbieter*“ auch die erforderlichen Berechtigungen aufgezählt: „BELW-GUTACHT“, „BELW-KURZBEW“ und „BELW-LAGBEUR“. Eine explizite Freigabeerklärung des Rechenzentrums liegt dem Prüfer jedoch nicht vor, ist unter dieser Berücksichtigung hier aber auch verzichtbar.

In den Abnahmen enthaltene Auflagen sind im Abschnitt *4.1* genannt.

Prüfinstitut

Die Prüfung wurde durchgeführt von Herrn König, Mitarbeiter des Informatikzentrums der Sparkassenorganisation GmbH (SIZ), Bonn.

1.9 Projektverlauf

- Das Projekt LORA Sparkassen Edition wurde mit der Beauftragung durch die Berlin Hyp anhand von Fachkonzepten und Prototyp 2004 gestartet.
- Folgeentwicklungen ab 2005 unter Einbindung stetig wachsender Nutzertreffen. Bei diesen Nutzertreffen werden sinnvolle Neuerungen von den Nutzern als auch von on-geo vorgeschlagen und per Protokoll zum Nutzertreffen für eine Realisierung beschlossen. Zur Vorversion 2.1 wurde in der Vergangenheit das Protokoll eines Nutzertreffens aus Weimar vorgelegt.
- Wesentliche Neuerungen in der hier betrachtenden Version sind in einem eigenen Kapitel der Benutzerhandbücher beschrieben (z. B. [109, 6.3 Änderungen der Version 2.4.2]).
- Die Herstellerinterne Testphase dieser neuen Version und führte am 03.06.2013 zur Herstellerfreigabe seitens des Herstellers [158].
- Im Rahmen der in diesem Dokument beschriebenen Prüfungsmaßnahmen hat das SIZ am 14.09.2012 den generellen Prüfauftrag erhalten (siehe [IDW EPS 460nF, Tz14ff]).
- Die erste Prüfungsphase durch das SIZ wurde durch den Auftrageber durch die Bereitstellung der prüfungsrelevanten Unterlagen (siehe Abschnitt *3 Literaturverzeichnis (inkl. Angaben zum geprüften Projekt)*) am 20.02.2013 begonnen. Diese Phase wurde nach interner Qualitätssicherung (siehe Historie dieses Dokumentes) durch eine am 14.03.2013 dem Auftraggeber übergebene Befundliste abgeschlossen.



- Seitens Hersteller nachgelieferte und überarbeitete Unterlagen wurden in der Prüfung berücksichtigt.
- In Absprache zwischen Auftraggeber und SIZ wurde im April 2013 beschlossen, den aktuellen Stand im Prüfbericht festzuhalten, dieses wurde nach interner Qualitätssicherung auch mit dem Auftraggeber abgestimmt und im Juni 2013 dem Auftraggeber übergeben.

2 Details zur Risikoklassifizierung

Die Risikokategorie für die gesamte Anwendung ergibt sich aus dem Maximum der potenziellen Auswirkungen. Es müssen alle fünf folgenden Abschnitte berücksichtigt werden [28,9].

Die folgende Tabelle benennt Unternehmensinteressen und verweist auf jeweils die spezifischen Risiken, durch die dieses Interesse gefährdet wird. Auf die Details wird dann in den folgenden Abschnitten eingegangen.

Unternehmens-interesse[4]	**Gefährdendes Risiko und Verweis auf konkrete Ausprägungen**[5]
Effektivität Effizienz [ISO/IEC 9126]	Auch wenn die IT-Anwendung bei Routinearbeiten sicher eine Unterstützung darstellt, geht das SIZ davon aus, dass der zeitliche Anteil einer Immobilienbewertung, der durch diese IT-Anwendung direkt beeinflusst wird im Verhältnis zu Gesamtzeit und Aufwand kaum signifikant ist und die Bewertungsmaßnahmen auch ohne diese Anwendung durchgeführt werden könnten und dabei im Verhältnis nur geringfügig länger dauern würden.
Vertraulichkeit	An die Vertraulichkeit der hier verarbeiteten Daten sind nach Ansicht des SIZ nur normale Anforderungen zu stellen. Eine Veröffentlichung der Daten und Ergebnisse sollte im Interesse von Immobilienbesitzern verhindert werden. Es sind in der Anwendung aber keine Informationen erkennbar, die nicht auch in öffentlichen Unterlagen enthalten sind oder auch durch in Augenscheinnahme des Objektes grob abgeschätzt werden können.
Integrität	Erstellte Gutachten dürfen nachträglich nicht änderbar sein, dies gilt primär aber für die außerhalb der Anwendung liegenden unterschriebenen Exemplare. Wichtiger als die Integrität der Gutachten ist die Integrität der in der IT-Anwendung enthaltenen Protokollfunktion zu bewerten. Diese Themen werden im Abschnitt *2.3 Auswirkungen auf das Sicherheitsniveau* behandelt.
Verfügbarkeit	Spezifische und als höher einzustufende Anforderungen an die Verfügbarkeit der IT-Anwendung können vom SIZ nicht gesehen werden.

[4] Unternehmensinteressen sind im „COBIT-Würfel“ [COBIT4.0, S.26] :, [COBIT4.1, S.25]:als Unternehmensanforderung beschrieben.

[5] Entsprechend [GAIT, Prinzip1] muss die übergeordnete Analyse von Risiken durchgeführt werden, bevor die in den Unterabschnitten im Rahmen der Analyse auszufüllenden Listen potenzieller Risiken bearbeitet werden.



Unternehmens-interesse[4]	**Gefährdendes Risiko und Verweis auf konkrete Ausprägungen[5]**
Compliance / Einhaltung rechtlicher Erfordernisse	Kreditvergabe und damit die Sicherheitsbewertung hier konkret von Immobilien müssen gesetzlichen und institutionellen Vorgaben entsprechen. Das Einhalten dieser Vorgaben muss auch nachträglich überprüfbar werden. Hierbei leistet die IT-Anwendung durch die Historisierung der im Rahmen einer Immobilienbewertung durchgeführten Aktionen wertvolle Hilfestellung. Diese Themen werden in den Abschnitten *2.1 Wirtschaftliche Auswirkungen bzw. Auswirkungen auf geschäftspolitische Entscheidungen*, *2.3 Auswirkungen auf das Sicherheitsniveau* und *2.4 Einhaltung gesetzlicher oder bankaufsichtsrechtlicher Vorschriften* behandelt.
Verlässlichkeit	Spezifische und als höher einzustufende Anforderungen an die Verlässlichkeit der IT-Anwendung können vom SIZ nicht gesehen werden.

LORA **stellt nach der in diesem Dokument beschriebenen Risikobeurteilung eine IT-Anwendung mit einem durch das SIZ nicht final bewertbarem Risiko dar.**

Um die in einem Institut erforderliche Bewertung zu vereinfachen sind die Teilaspekte aus Sicht des SIZ nachfolgend beschrieben.

Ausschließlich um einem einsetzenden Institut alle Risikohöhen bei der Bewertung und der folgenden Einsatzfreigabe durch das Institut zu ermöglichen, wird die Prüfung sicherheitshalber unter der Annahme der potenziell möglichen Risikostufe A nach OPDV 1-2006 durchgeführt. Diese Aussage hat keinen Empfehlungscharakter hinsichtlich der vom Institut angenommenen Risikohöhe.

2.1 Wirtschaftliche Auswirkungen bzw. Auswirkungen auf geschäftspolitische Entscheidungen

Die IT-Anwendung unterliegt folgenden Beurteilungskriterien zu wirtschaftlichen Auswirkungen:

- Die IT-Anwendung ist über die Bewertung von Immobilien und damit Sicherheiten sowohl in die Kreditvergabeprozesse als auch die damit verbundenen Folgeprozesse eingebunden. Allein das hieraus resultierende Risiko berechtigt die Vergabe einer hohen Risikostufe (Kategorie A nach OPDV 1/2006), siehe hierzu aber auch Abschnitt 2.4. Das hier genannte Risiko wird durch den manuellen Qualitätssicherungsprozess auf den erstellten Gutachten signifikant reduziert, dessen Auswirkung muss durch das einsetzende Institut bewertet werden.
- Das Operative Risiko durch den IT-Lieferanten [IIR2, 20] wird dadurch reduziert, dass es mit Produkten anderer Dienstleister auch Alternativen gibt.

Andere wirtschaftliche Auswirkungen oder Auswirkungen auf geschäftspolitische Entscheidungen werden nicht gesehen. Insgesamt lassen sich dabei die wirtschaftlichen Auswirkungen durch die IT-Anwendung vom SIZ nicht final bewerten.



2.2 Auswirkungen auf die Kundenbeziehung

Die IT-Anwendung unterliegt folgenden Beurteilungskriterien zu Auswirkungen auf die Kundenbeziehung:

- Neben den bereits im obigen Abschnitt genannten Auswirkungen auf Kreditvergaben, die irgendwann auch auf den Sparkassenkunden wirken, kann das SIZ hier keine spezifischen Auswirkungen erkennen. Dieser Kunde sieht nur die von diversen Mitarbeitern gelieferten Kreditaussagen und damit keine Ergebnisse der IT-Anwendung.
- Als Sonderfall der Auswirkungen auf Kundenbeziehungen muss die Gutachtenerstellung im direkten Auftrag für einen Kunden gesehen werden, bei der das erstellte Gutachten im Anschluss an den Kunden herausgegeben wird. Diese Gutachten sind aber zu unterschreiben und stellen nicht die Kernaufgabe eines Kreditinstitutes dar.

Auswirkungen auf die Kundenbeziehung werden nicht gesehen, da die Informationen nur Institutsintern vorgelegt, nicht aber Richtung Sparkassenkunden kommuniziert werden.

2.3 Auswirkungen auf das Sicherheitsniveau

Die IT-Anwendung unterliegt folgenden Beurteilungskriterien zu Auswirkungen auf das Sicherheitsniveau:

- Die notwendige Verfügbarkeit [IIR2, 20 Datenverarbeitungsrisiken: Verfügbarkeit] von *LORA* wird aus Sicht des SIZ mit mehrmals wöchentlich als sehr niedrig eingeschätzt, alle betroffenen Teilprozesse wären darüber hinaus auch ohne diese Anwendung bearbeitbar.
- Zur Sicherstellung der erforderlichen Integrität der Informationen ist eine ausreichende Funktionstrennung (Segregation of Duties) in der Bedienung der IT-Anwendung erforderlich. Diese wird im Rahmen der Immobilienbewertungen durch eine ausreichende Anzahl von manuellen Unterschriften auf den Reports sichergestellt.
- Das Verfahren zur Verschlüsselung der mit dem Gutachter ausgetauschten Daten ist mit einer symmetrischen Rijndael-Verschlüsselung mit 128bit Verschlüsselung [152, 2.1.6 Externe Gutachter] beschrieben. Wikipedia benennt keine aktuellen aber denkbare zukünftige erfolgreiche Angriffsszenarien [157].
- Sofern die IT-Anwendung innerhalb der im vorliegenden Prüfbericht angesprochenen Grenzen betreiben wird, d. h. ohne Zugriff auf on-geo-Server (zur Vervollständigung der Daten), liegen alle schützenswürdigen Informationen entweder in der Datenbank oder in zu verschlüsselnden Dateien und lassen sich unter Zuhilfenahme der Dokumentation ausreichend schützen.

Im Rahmen der Risikobewertung sind die Auswirkungen auf das Sicherheitsniveau zu bestimmen, die sicher von Institut zu Institut unterschiedlich sind. Allen gemeinsam dürfte aber sein, dass für diese IT-Anwendung, wenn sie im benannten Umfang betrieben wird, im Wesentlichen sicher zu stellen ist, dass Anwender zwar ihre Anwendung aufrufen dürfen, aber keinen weitergehenden Schreibzugriff auf die zentrale Datenbank haben dürfen. Auch die anderen sicherheitstechnisch relevanten Aspekte, sie sind im Sicherheitshandbuch beschrieben, stellen für einen üblichen Administrator keine speziellen Anforderungen dar und liefern dabei auch keine Auswirkungen.

Andere Auswirkungen auf das Sicherheitsniveau werden nicht gesehen. Insgesamt werden dabei diese Auswirkungen durch die IT-Anwendung vom SIZ als minimal bewertet.



2.4 Einhaltung gesetzlicher oder bankaufsichtsrechtlicher Vorschriften

Die IT-Anwendung unterliegt folgenden Beurteilungskriterien zu Auswirkungen auf die Einhaltung von gesetzlichen und sonstigen relevanten Vorschriftenn, einschließlich dem Internen Kontrollsystem (IKS):

- Das Vorhandensein ausreichender und berechtigter Unterschriften auf den Immobilienbewertungsberichten kann außerhalb der IT-Anwendung überprüft werden.
- Die Protokollierung der im Rahmen einer Immobilienbewertung durchgeführten Schritte ist in der Anwendung einsehbar. Beschreibungen dazu finden sich in den Handbüchern.
- Die zur Verhinderung einer Protokollveränderung durch unberechtigte Mitarbeiter notwendigen Schritte sind im Sicherheitshandbuch zu LORA ausreichend beschrieben.

Da die Bewertung der Immobilien als Bestandteil der dem Kreditprozess zuzurechnenden Sicherheitenbewertung einem aufsichtsrechtlichen Kernprozess des Finanzinstitutes zuzurechnen ist, kann dies allein als ausreichend für ein hohes Risiko angesehen werden und unterliegt damit der Risikokategorie A nach OPDV 1/2006. Sowohl die Bewertung selbst als auch die hierzu erforderliche Qualitätssicherung werden aber auf Basis nachvollziehbarer Dokumente durchgeführt, die in beiden Fällen manuell zu unterschreiben sind. Es ist damit auch zulässig den Risikoanteil der IT-Anwendung LORA Sparkassenedition als nicht mehr signifikant und damit in die Kategorie C nach OPDV 1/2006 einzustufen.

Die Liste der einzuhaltenden Vorgaben bestimmt sich nicht nur aus gesetzlichen Vorgaben wie *§77 InvG - Sachverständigenausschuss*[6]*, §16 PfandBG – Beleihungswertermittlung, §6 BelWertV – Gutachter* und *§ 12 BelWertV - Kapitalisierung der Reinerträge*[7] sondern auch aus Vorgaben des jeweiligen Institutes. Diese Vorgaben müssen aber primär durch die entsprechenden Mitarbeiter umgesetzt und im Rahmen der Qualitätssicherung überwacht werden. Die IT-Anwendung und damit das von ihr ausgehende Risiko spielen bei der Einhaltung dieser Vorgaben eine eher untergeordnete Rolle.

Andere Auswirkungen auf gesetzliche oder andere relevante Vorgaben werden nicht gesehen. Insgesamt werden dabei diese Auswirkungen durch die IT-Anwendung vom SIZ als nicht final bewertbar festgestellt.

2.5 Datenüberstellung in autorisierte Programme

Eine Datenüberstellung nach OSPlus findet statt, eine inhaltliche Beschreibung der Schnittstelle wurde vorgelegt [155]. Eine echte Abnahme der Finanz Informatik (FI) wurde dem SIZ nicht vorgelegt, die Prüfer wertet hier ersatzweise die Organisationsrundschreiben der FI als Abnahme, siehe Abschnitt *1.8 Projektbeteiligte*.

Eine Datenüberstellung in weitere Programme, wie z. B. ELAXY [153, LORA Immobilienplattform], wird durch diesen Prüfbericht nicht autorisiert. Da die Daten aber sowohl in einem Word-Excel-Gemisch auf Anwenderseite als auch in der Datenbank mit einem ggf. auch ausgelieferten Datenmodell auf Betreiberseite verfügbar wären, kann eine Verwendung der Daten für andere Zwecke nicht ausgeschlossen werden.

Zu LORA werden spezielle Module zum Export in andere Anwendungen geliefert, die ebenfalls diesem Ausschluss unterliegen, wie die Schnittstelle in die VDP-Transaktionsdatenbank [131].

---

[6] Ähnliche Vorgaben finden sich auch in §10 KWG (4b) .

[7] Der §12 der BelWertV kann hier nur als Beispiel genannt werden, inhaltlich stellen große Teile dieser Verordnung inhaltliche Anforderungen an ein Immobiliengutachten.



Andere Datenübermittlungen werden nicht gesehen. Insgesamt lassen sich dabei die Auswirkungen bei Nutzung der OSPlus-Schnittstelle durch die IT-Anwendung als hoch (Risikostufe A) bewerten.

3 Literaturverzeichnis (inkl. Angaben zum geprüften Projekt)

Im Testierungsprojekt wurden u. a. folgende Artefakte[8] vollständig berücksichtigt, im Dokument selbst werden weitere Referenzen durch eckige Klammern gekennzeichnet und dabei jeweils die verständliche Kurzbezeichnung des Dokumentes angegeben, z. B. [HGB, §238]:

[2] Arbeitshilfe für die Beurteilung von Qualitätseigenschaften bei Fremdsoftware (Erstveröffentlichung: Fachmitteilungen Nr. 7 vom 31. 3. 1999 durch den Fachausschuss OPDV, Anm. d. Red.)

[3] DIN ISO/IEC 12119 „Software-Erzeugnisse, Qualitätsanforderungen und Prüfbestimmungen"

[4] [GoBS] Grundsätze ordnungsgemäßer DV-gestützter Buchführungssysteme - Schreiben des Bundesministeriums der Finanzen an die obersten Finanzbehörden der Länder vom 7. November 1995, veröffentlicht im BStBl. 1995, Teil I, S.738ff.

[8] TÜViT im Rahmen der Überarbeitung der Checkliste für das Projekt TRAVIC Jan 2005

[16] AE-Modell des SIZ

[19] [= FAIT1] IDW-Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW RS FAIT 1); (Stand: 24.09.2002): Verabschiedet vom Hauptfachausschuss (HFA) am 24.09.2002

[28] SVN Prüfungsstellen, Checkliste für IT-Prüfungen, CL Softwarebeschaffung.doc

[39] REVISIONSSYMPOSIUM NEUE ZIELE - NEUE WEGE FÜR DIE INTERNE REVISION 23. und 24. April 2008 in Bad Homburg v. d. Höhe
Vortrag: Auslagerungen von Geschäftsbereichen im Fokus der Internen Revision; Dr. Josef Kokert, Bundesanstalt für Finanzdienstleistungen

[49] DSGV Rundschreiben 2009/209 Anlage 1: Fachausschuss Ordnungsmäßigkeit und Prüfung der Datenverarbeitung (OPDV) - Stellungnahme Nr. 1/2009 (Risikoorientierte Steuerung und Überwachung der Auslagerung von IT-Services)

[54] Bundesministerium für Wirtschaft und Technologie, Dokumentation 564, Handlungsleitfaden zur Aufbewahrung elektronischer und elektronisch signierter Dokumente, Stand August 2007

[103] White Paper LORA Speed 2.4 – Produktbeschreibung, November 2012
06.11.2012 14:09 165.533 \130220 E Unterlagen\113_WhitePaper_LORA_Speed_2.4.pdf

[104] on-geo Allgemeine Pflegebedingungen für lizenzierte Softwareprogramme und Immobilienplattform (Stand 25.03.2010)
16.10.2012 11:34 46.415 \130220 E Unterlagen\121_Allgemeine_Pflegebedingungen.pdf

[105] Hinweise zu Wartung und Pflege für LORA-Software, Stand 15.11.2004
30.11.2004 16:42 361.854 \130220 E Unterlagen\122_Hinweise_zur_Wartung_LORA.pdf

[8] Berücksichtigte Artefakte (SW-Teile und Dokumente) werden in den Testierungsdokumenten mit abkürzender Notation der Quelle hier mit [<lit-nr>] bezeichnet, wenn dieses Artefakt im Literaturverzeichnis auftaucht. Konkrete Inhalte innerhalb dieser Quelle werden dabei möglichst auch detaillierter angegeben:
[<lit-nr>, <Abschnitt>] Der Abschnitt kann dabei auch aus der Abschnittsnummer gebildet werden
[<lit-nr>, S.<Seitennummer>] Als Seitenangabe im Dokument
[<lit-nr>, XYZ] wenn XYZ in der speziellen Dokumentenform eine Stelle eindeutig kennzeichnet, bei Tabellenkalkulationsprogrammen z. B. die Zellennummern.
Für allgemein bekannte Literaturhinweise wird statt der numerischen Angabe auch die abkürzende Bezeichnung im Text verwendet, auch wenn dieses Schriftstück nicht im Literaturverzeichnis auftaucht.

[106] Allgemeine Bestimmungen zur Softwareüberlassung für die LORA-Immobilienplattform, LORA-Gutachterlösung, LORA-Besichtigerlösung und LORA-Wertschätzerlösung (Stand 01.03.2010)
16.10.2012 11:34 66.334 \130220 E Unterlagen\131_Allgemeine_Bestimmungen_zur_Softwareueberlassung.pdf

[107] Allgemeine Geschäftsbedingungen on-geo GmbH, Stand: 15.02.2011
16.10.2012 11:33 70.276 \130220 E Unterlagen\132_Allgemeine_Geschaeftsbedingungen_ongeo.pdf

[108] Preisliste LORA Sparkassen on-geo 2013, Stand: 31.01.2013
31.01.2013 08:16 26.982 \130220 E Unterlagen\141_Preisliste LORA Sparkassen.pdf

[109] Benutzerhandbuch LORA Sparkassen Edition dual 2.4, © 2012
10.08.2012 12:46 13.092.961 \130220 E Unterlagen\211_Benutzerhandbuch Lora Sparkassen Edition 2.4.pdf

[110] Erste Schritte LORA Sparkassen Edition 2.4, © Copyright on-geo GmbH 2012
20.07.2012 09:18 9.137.484 \130220 E Unterlagen\212_Erste Schritte LORA Sparkassen Edition 2.4.pdf

[119] Installationsanleitung LORA Sparkassen Edition 2.4, LORA Speed 2.4
13.03.2013 09:24 4.046.590 \130314 E Nachliefe-rung\231a_Installationsanleitung_LORA_ Sparkassen_Edition_2.4.pdf
13.03.2013 09:24 3.958.098 \130314 E Nachliefe-rung\231b_Installationsanleitung_LORA_Speed_2.4.pdf

[122] Betriebshandbuch LORA Sparkassen Edition 2.4, Oktober 2012
17.10.2012 09:13 112.578 \130220 E Unterlagen\242_Betriebshandbuch LORA Sparkassen Edition 2.4.pdf

[126] LORA Speed und MBWR Onlinedatensatz, August 2012
09.11.2012 12:22 162.914 \130220 E Unterlagen\2503_LORA Speed und MBWR Onlinedatensatz.pdf

[129] Muster Ausdruck Kurzgutachten LORA Speed für Eigentumswohnung und Einfamilienhaus
05.06.2012 12:52 105.194 \130220 E Unterlagen\2506_Muster Ausdruck Kurzgutachten LORA Speed für EFH.pdf
05.06.2012 12:55 90.214 \130220 E Unterlagen\2506_Muster Ausdruck Kurzgutachten LORA Speed für ETW.pdf

[131] Export VDP- Transaktionsdatenbank für LORA 2.4, Oktober 2012
21.01.2013 17:05 91.781 \130220 E Unterlagen\2508_Export VDP-Transaktionsdatenbank für LORA Speed 2.4.pdf

[137] LORA Entwicklungsprozess und Qualitätssicherung, Oktober 2012
13.03.2013 09:24 119.370 \130314 E Nachliefe-rung\311_LORA_Entwicklungsprozess_Qualitätssicherung.pdf

[140] Feinkonzept LORA Speed Wartungsrelease 2011, Februar 2013 LORA-Version 2.4
19.02.2013 11:46 1.269.711 \130220 E Unterlagen\3202_Feinkonzept LORA Speed WR2011.pdf

[141] Feinkonzept Anpassungen LORA Speed PPU Februar 2013 LORA-Version 2.4
05.02.2013 14:39 1.354.805 \130220 E Unterlagen\3203_ Feinkonzept PPU.pdf

[142] LORA Edition Änderungen Erbbaurecht Februar 2012
08.02.2012 15:35 427.173 \130220 E Unterlagen\3204_LORA Edition Erbbaurecht.pdf

[143] Grobkonzept LORA Abruf von Besichtigungen und weiteren Researchdaten über LORA Februar 2013 LORA-Version 2.4 (Einfacher Abruf von Researchdaten)
19.02.2013 14:50 310.620 \130220 E Unterlagen\3205_Abruf_Researchdaten.pdf

[144] Feinkonzept Überarbeitung Terminverfolgung Februar 2013 LORA-Version 2.4
19.02.2013 16:07 644.466 \130220 E Unterlagen\3206_LORA_Feinkonzept_Terminverfolgung.pdf

[145] Testzusammenfassung LORA Enterprise WR2011 (Rxx), Releasenummer bis 2.4.2.0.9
12 03 Testanweisungen LORA Enterprise WR2011: R01 bis R09
31.01.2013 16:09 4.567.468 \130220 E Unterlagen\3301_Testanweisung LORA Enterprise WR2011 R01.pdf
31.01.2013 16:31 2.293.262 \130220 E Unterlagen\3302_Testanweisung LORA Enterprise WR2011 R02.pdf
01.02.2013 10:34 657.182 \130220 E Unterlagen\3303_Testanweisung LORA Enterprise WR2011 R03.pdf
01.02.2013 11:43 2.550.227 \130220 E Unterlagen\3304_Testanweisung LORA Enterprise WR2011 R04.pdf
05.02.2013 09:41 1.853.022 \130220 E Unterlagen\3305_Testanweisung LORA Enterprise WR2011 R05.pdf
05.02.2013 09:55 62.446 \130220 E Unterlagen\3305_Testanweisung LORA Enterprise WR2011 R06.pdf
05.02.2013 10:06 49.581 \130220 E Unterlagen\3306_Testanweisung LORA Enterprise WR2011 R07.pdf



05.02.2013 10:47 417.953 \130220 E Unterlagen\3307_Testanweisung LORA Enterprise WR2011 R08.pdf
05.02.2013 13:20 642.457 \130220 E Unterlagen\3308_Testanweisung LORA Enterprise WR2011 R09.pdf

[147] Testprotokoll, LORA Sparkassen Edition Produktversion: u.a. 2.4.2.0.9
Testprotokoll LORA Enterprise WR2011: R01 bis R09
09.11.2012 09:56 4.509.584 \130220 E Unterlagen\3401_Testprotokoll LORA Enterprise WR2011 R01.pdf
09.11.2012 09:50 2.258.582 \130220 E Unterlagen\3402_Testprotokoll LORA Enterprise WR2011 R02.pdf
09.11.2012 09:51 668.136 \130220 E Unterlagen\3403_Testprotokoll LORA Enterprise WR2011 R03.pdf
09.11.2012 10:39 2.552.236 \130220 E Unterlagen\3404_Testprotokoll LORA Enterprise WR2011 R04.pdf
09.11.2012 10:48 2.013.110 \130220 E Unterlagen\3405_Testprotokoll LORA Enterprise WR2011 R05.pdf
09.11.2012 10:56 61.573 \130220 E Unterlagen\3406_Testprotokoll LORA Enterprise WR2011 R06.pdf
09.11.2012 11:09 54.880 \130220 E Unterlagen\3407_Testprotokoll LORA Enterprise WR2011 R07.pdf
09.11.2012 11:07 420.633 \130220 E Unterlagen\3408_Testprotokoll LORA Enterprise WR2011 R08.pdf
09.11.2012 11:12 814.325 \130220 E Unterlagen\3409_Testprotokoll LORA Enterprise WR2011 R09.pdf

[149] Betriebshandbuch LORA Sparkassen Edition 2.4, März 2013
26.03.2013 09:32 390.457 \130326 E Nachlieferung\130324_Betriebshandbuch_LORA_Sparkassen_Edition_2.4_Änderungen.pdf

[151] Ergänzung Bestellung Handelsplattform
26.03.2013 09:32 280.176 \130326 E Nachlieferung\130325_Ergänzung_Handelsplattform.pdf

[152] Sicherheitshinweise LORA Sparkassen Edition LORA 2.4, März 2013
26.03.2013 09:32 583.371 \130326 E Nachlieferung\130325_Sicherheitshinweise_LORA Sparkassen_Edition_2.4.pdf

[153] LORA Sparkassen Edition Version 2.4, White Paper Produktbeschreibung November 2013, Stand: März 2013
26.03.2013 09:32 860.110 \130326 E Nachlieferung\130325_WhitePaper_LORA_Sparkassen_Edition_2.4_Änderungen.pdf

[155] Dokument zum Datenaustausch an der Schnittstelle zu OSPlus vom 26.04.2013 (Das Dokument hat keinen expliziten Titel)
26.04.2013 15:23 372.405 \130429 E Nachlieferung\130426_Datenaustausch_OSPlusSchnittstelle.pdf

[156] on-geo Application Service Providing
http://www.on-geo.de/is-cms/index.php?id=85

[157] Advanced Encryption Standard
http://de.wikipedia.org/wiki/Rijndael

[158] Herstellerfreigabe

4 Zusammenfassende Bewertung der IT-Anwendung aus Sicht der Stellungnahmen

<table>
<tr><th colspan="4">Programmfreigabeerklärung
(ähnlich Anlage 2 zur Stellungnahme Nr. 1/2006 des Fachausschusses OPDV)</th></tr>
<tr><td>Ausreichend erfüllt</td><td colspan="2">Thema / Unterthema</td><td>Details siehe Abschnitt</td></tr>
<tr><td></td><td colspan="2">Projektverantwortung, Erklärung zur Projektleitung</td><td>5</td></tr>
<tr><td></td><td colspan="2">Benutzer / Fachbereiche,</td><td>6</td></tr>
<tr><td></td><td></td><td>Es muss sichergestellt sein, dass die fachlichen Anforderungen erfüllt wurden</td><td>6.1</td></tr>
<tr><td></td><td></td><td>Es muss sichergestellt sein, dass die gesetzlichen Anforderungen erfüllt wurden</td><td>6.2</td></tr>
<tr><td></td><td></td><td>Die Funktionsfähigkeit [ISO/IEC 9126] muss durch Test nachgewiesen worden sein</td><td>5.3</td></tr>
<tr><td></td><td></td><td>Es muss sichergestellt sein, dass eine übersichtliche und vollständige Benutzerdokumentation übergeben wurde</td><td>6.3</td></tr>
</table>



Programmfreigabeerklärung (ähnlich Anlage 2 zur Stellungnahme Nr. 1/2006 des Fachausschusses OPDV)			
Ausreichend erfüllt	Thema / Unterthema		Details siehe Abschnitt
	Produktion, Erklärung zur (EDV-/IT-) Organisation		7
		Es muss sichergestellt sein, dass der erforderliche Sicherheitsstandard nicht unterlaufen wird	7.4

Der Prüfer empfiehlt damit die Programmfreigabe nach OPDV 1-2006.

4.1 Auflagen

Im Betrieb sind die folgenden Auflagen einzuhalten.

- **Im Sicherheitshandbuch** [152] **genannte Aspekte sind umzusetzen**.
- **Berechtigungen auf der zentralen Dateiablage müssen durch den Betreiber geklärt und umgesetzt werden**, siehe Abschnitt *5.2.1 Anforderungserfassung (AE)*. Das Sicherheitshandbuch [152, 2.1.5 Zentrale Dateiablage Zugriffsrechte] macht auf diese Notwendigkeit aufmerksam, das während der Prüfung überarbeitete Betriebshandbuch [149, zentrale Dateiablage] spezifiziert Unterordner mit potenziell unterschiedlich zu vergebenden Berechtigungen. Einen Hinweis auf die Notwendigkeit des Schrittes liefert auch das Sicherheitshandbuch [152, 2.1.5 Zentrale Dateiablage Zugriffsrechte] mit „*Bitte klären Sie mit der Organisation, für welche Daten die zentrale Dateiablage von LORA genutzt werden soll und welche Schutzmaßnahmen sich daraus ergeben*". Potenziell müssen mehrere Bereiche eingerichtet werden.
- **Accountdaten für Datenbankzugriff und Onlinezugriffe sind** manuell **zu verschlüsseln**. Das Sicherheitshandbuch [152, 2.1.4 Zugriffsschutz für Datenbank und Online-Dienste] benennt den Einsatz eines entsprechenden Verschlüsselungstools, Details siehe Abschnitt *7.4.3 Key- Management (K108)*.
- **Die im für das jeweilige on-geo-Produkt mitgelieferten Dokument „Erste Schritte <*Produktname*>" genannten Anforderungen sind umzusetzen.**
- **Sowohl die eigentliche Auftragsvergabe an externe Gutachter als auch die erforderliche Archivierung der Handelsbriefe sind manuell durch den LORA-Anwender sicher zu stellen** und werden durch die IT-Anwendung nicht geleistet, siehe auch Abschnitte *6.2.2 BGB* und *6.2.6 HGB*. Potenziell können dabei auch die Abschnitte *6.2.14.1 Stellungnahme Nr. 1/1997 Besondere Ordnungsmäßigkeitsanforderungen bei elektronischer Archivierung/Aktenführung* und *6.2.15.1 IDW RS FAIT 3, IDW Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung beim Einsatz elektronischer Archivierungsverfahren* relevant werden.
- **Speicherung, Verarbeitung und potenzielle Weitergabe von Immobiliendaten an externe Gutachter unterliegen dem BDSG und müssen vom Institutskunden und vom DSB genehmigt sein**, siehe auch Abschnitt *6.2.3 BDSG*. **Für den Datenschutz beim Gutachter ist hinsichtlich der vertraglichen Regelungen das beauftragende Institut verantwortlich**, siehe auch Abschnitt *8 Detailbewertung bei ganz oder teilweise ausgelagertem Betrieb*.
  Diese Verantwortungen erstrecken sich auch auf den Supportvertrag und ein potenzielles Hosting oder die Verwendung anderer Dienstleistungen des Herstellers.



- **Warnhinweise aus der Anwendung tauchen nur dann im Gutachten auf, wenn die entsprechenden Vorlagen korrekt definiert sind**, siehe auch Abschnitt *6.2.5 GPSG*.
- Die **LORA-Anwendungen sind <u>nicht</u> für rechnungslegungsrelevante Geschäftsprozesse freigegeben**, siehe auch Abschnitt 6.2.10 AO (Abgabenordnung und Aufbewahrungsfristen), GoBS und Verarbeitung buchungsrelevanter Geschäftstransaktionen. **Dies gilt auch für in der Produktbeschreibung genannte Funktionen** [153, Druck Auftrag, Rechnung und Laufzettel].
- **Für die nach §24 BelWertV erforderliche Stichprobenkontrolle ist die korrekte Ermittlung der Stichprobengröße durch den Institutsmitarbeiter durchzuführen**, siehe auch Abschnitt *6.2.11 BelWertV*.
- **Es ist eine aus Institutssicht korrekte Kontrolle der erstellten Gutachten zu definieren und in LORA zu konfigurieren**, Details finden sich im Abschnitt *5.2.2.2 Integration in den Geschäftsprozess*.
- **Für die Übermittlung der nach Releasewechseln ggf. geänderten Vorlagen an die beauftragten Gutachter ist** allein **das einsetzende Institut verantwortlich**, siehe auch Abschnitt *5.4.1 Versionsverwaltung und Identifikation*.
- Die Nutzung von Reseachdaten wurde in LORA integriert und ist im Auslieferungszustand „eingeschaltet“ und widerspricht damit den Aussagen des folgenden Abschnittes. **Im Institut ist** damit **festzulegen, ob Reseachdaten** tatsächlich **eingeschaltet bleiben dürfen oder manuell ausgeschaltet werden müssen**. Nach Testkonzept [145, R06] kann der *Sofortabruf aus LORA … über einen Stammdatenschalter an- und abgeschaltet werden*.
- **Institutsmitarbeiter sind auf urheberrechtliche Betrachtung von Fotos und anderem Material** über Immobilien **bei der Nutzung** dieser Informationen bei einer Immobilienbewertung **hinzuweisen**, näheres siehe Abschnitt *6.2.8 UrhG*.

4.2 Verwendung von Researchdaten

Mit dem vorliegenden Prüfbericht wird <u>keine</u> Programmfreigabe für die Verwendung von kostenpflichtigen Researchdaten und potenziell darüber hinausgehenden Geschäften auf der Handelsplattform des Herstellers [107, 2 Zugangs- und Teilnahmeberechtigung (2)] erteilt. Sollte dies für ein Finanzinstitut trotzdem relevant sein, müssen individuell mindestens folgende Fragestellungen gelöst werden:

- Die Bereitstellung von Researchdaten erfolgt gegen Berechnung, d. h. auf der Basis sowohl eines Rahmenvertrages als auch eines Einzelbereitstellungsvertrages –letzterer innerhalb der IT-Anwendung. Eine Konformität der IT-Anwendung mit [BGB, §145ff] und [BGB, §241ff] müsste erst noch festgestellt werden.
- In den dem Institut gelieferten Researchdaten sind auch Bewertungen enthalten die zu 75% direkt aus der Adressinformation und fast der komplette Rest indirekt daraus abgeleitet werden [126, 2.2 Lage/ Standort (für Wohnen)]. Eine Konformität der IT-Anwendung mit [BDSG, §28a Datenübermittlung an Auskunfteien], [BDSG, §28b Scoring] und [BDSG, §29 Geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung] müsste erst noch festgestellt werden, siehe auch Abschnitt *8.1.2 §11 BDSG, §§241,311 BGB - Datenschutz*.
- Für den Zugriff auf die Researchdaten sind Schnittstellen beim Provider vorhanden. Die ausreichende Sicherheit dieser Schnittstellen müsste erst noch festgestellt werden.



- Dem SIZ wurde ein Dokument „Ergänzung Bestellung Handelsplattform“ [151] ohne Versionszugehörigkeitsinformationen übergeben, nach dem eine nicht mit der PAngV kompatible Bestellung ausgelöst werden könnte, weitere Hinweise hierzu siehe Abschnitt *6.2.9 Verbraucherkreditrichtlinie*.
- Das Konzept zur Integration der Reseachdaten [143] befindet sich noch „in Erstellung“ und ist noch nicht abgeschlossen. Das Konzept [143, 2.4 Offene Fragen] sieht eine nur 30-tägige Archivierung vor und umfasst damit nicht die nach [HGB, §257] länger definierten Aufbewahrungspflichten für Bestellungen.
- Das Testprotokoll der Sparkassenedition behandelt auch den Test der Online-Plattform und stellt dabei signifikante Mängel fest [147, R09, S.16].

5 Detailbewertung der Bereitstellungs- und Wartungsprozesse (Projektverantwortung)

Ein Prozesshandbuch [137] mit den herstellerseitigen Bereitstellungsprozessen wurde vorgelegt und ist mit der beim Audit im Jahr 2007 vorgefundenen Situation hinsichtlich Ordnungsmäßigkeitskriterien kompatibel, stellt aber eine Weiterentwicklung der Prozesse dar.

5.1 Nachvollziehbares Projektmanagement

MaRisk [MaRisk, BTR 4 Operationelle Risiken] und COBIT [COBIT4.0, PO1.1], [COBIT4.0, AI2.10] fordern eine Ursachenanalyse bei auftretenden Fehlern. Der vom Hersteller vorgelegte Musterwartungsvertrag [104] umfasst diesen Teil der Dienstleistung jedoch nicht. Beide Vorgaben sind für Softwarehersteller allgemein nicht als verbindlich anzusehen, insofern kann hier dem einsetzenden Institut nur empfohlen werden, dies selbst vom Hersteller zu fordern.

5.2 Fehlerfreie Herstellung der IT-Anwendung

5.2.1 Anforderungserfassung (AE)

LORA speichert Daten aller Nutzer in einer „zentralen Dateiablage“. Die Struktur dieser Dateiablage ist im während der Prüfung überarbeiteten Bentriebshandbuch [149, zentrale Dateiablage] beschrieben. **Inwieweit Berechtigungen auf den gesamten Ordner oder auf dessen enthaltene Teilordner vergeben werden müssen, muss institutsspezifisch abgeklärt werden**. Zu beachten ist dabei, dass in diesem Ordner auch der Unterordner „print“ hinterlegt ist, der Druckvorlagen enthält, deren Änderungsmöglichkeit als kritisch einzustufen ist. Der Prüfer muss daher empfehlen, die Durckvorlagen an einem veränderungsgeschützten Ort aufzubewahren.

5.2.2 Architektur und Schnittstellendesign, Geschäftsprozessmodellierung (GPM)

5.2.2.1 Schnittstellen und sicherer Datenaustausch

Eine Beschreibung der Daten, die aus OSPlus nach LORA und zurück nach OSPlus überstellt werden, wurde vorgelegt [155].

Das Datenmodell [126] sind für einen Bertreiber verständlich beschrieben und lassen keine relevanten Probleme erkennen.

Die internen Dokumente aber auch die Betreiberbeschreibungen sind hinsichtlich der darin vorhandenen Benennungen nicht immer mit gesetzlichen oder normativen Vorgaben kompa-

tibel, da Begriffe verwendet werden, die aus externer Sicht eine andere Bedeutung besitzen, wie z. B. der Begriff Plausibilisierung.

Nach Testprotokoll [147, R02, 2.2 Dokumentation] ist die Sterbetafel 2008/2010 hinterlegt. Nach Aussagen des Herstellers ist zur Zeitpunkt der hier dokumentierten Prüfung keine aktuellere Sterbetafel verfügbar.

Die Übernahme von Daten in andere Anwendungen, z. B. durch Zugriff auf die LORA-Datenbank wird durch diesen Prüfbericht nicht legitimiert.

Für die potenzielle Nutzung der durch den Prüfbericht nicht legitimierten Internetschnittstellen von LORA (Researchdaten oder ausgelagerte Dienstleistungen) wäre ein sogenannter Penetrationstest erforderlich, der bislang nicht vorgelegt wurde.

5.2.2.2 Integration in den Geschäftsprozess

COBIT [COBIT4.0, AI2.3] fordert Kontrollen in der Anwendung und bei den Anwendern. Um dem Institut die entsprechenden Abgrenzungen zu erlauben, beschreibt das Benutzerhandbuch [109, 3.6 Plausibilisierung] für erforderlich gehaltene organisatorische Qualitätssicherungsprozesse und die erforderlichen Berechtigungen [107, 4.3.5.3 Stammdaten Nutzergruppen]. Eine technische Unterstützung der manuallen Qualitätssicherung ist in diversen Abschnitten jeweils unter der Unterüberschrift Plausibilisierung beschrieben. In vielen Fällen kann die Plausibilisierung durch Ändern der Stammdaten verändert werden, hierauf wird mit hingewiesen. **Es verbleibt damit Institutsaufgabe, eine aus Institutssicht korrekte Kontrolle zu definieren und in LORA zu konfigurieren**.

5.2.3 Programm- bzw. Systemdokumentation

Anwendungen verursachen ggf. neben der Anschaffung weitere Kosten, die zumindest transparent werden müssen. Die Preisliste [108] enthält dazu neben den Lizenz- und Wartungskosten auch Preisangaben zu Hosting oder den bereitgestellten Researchdaten.

Die Beschreibung der im Programm vorhandenen Abläufe muss vollständig sein [2, 1.3.2]. Neben Produktbeschreibung [153], Anwender- [109] und Betriebshandbuch [149] liegen Beschreibungen von mathematischen Verfahren [153] und einiger Beispielgutachten [129]. Dokumentationen zum Datenaustausch mit dem Gutachter, Beschreibungen des Berechtigungskonzeptes oder der integrierten Honorarberechnung wurde bei früheren Prüfungen vorgelegt und aktuell nicht weiter hinterfragt. Untransparent Abläufe sind seitens SIZ nicht identifizierbar.

5.3 Nachweis einer vollumfänglichen Qualitätssicherung

Siehe auch [SITB, K341(Test und Freigabe)].

5.3.1 Nachweischarakter von Testergebnissen

Seitens on-geo wurden Testprotokolle [145] und [147] vorgelegt. Hinsichtlich der Nachweisfunktion werden diese Dokumente folgender Maßen durch das SIZ bewertet:

- Sie bestätigen, dass einige Funktionen im Bereich Researchdatenverwendung nicht vollständig wie erwartet funktionieren. Die Existenz dieser Probleme belegt die Korrektheit der Unterlagen bleibt für die Freigabe aber ohne negative Auswirkungen, da die Verwendung von Reseachdaten nicht durch den Prüfbericht legitimiert wird.
- Sie dokumentieren geringere Programmfehler in der LORA-SparkassenEdition bei Auswertungen und Auftragserstellungen durch Kopie und bestätigt damit, dass eine korrekte Handhabung der Anwendung erforderlich ist. Da sich die Fehler



aber nur auf das Handling nicht aber direkt auf die Ergebnisse auswirken, bleiben diese Fehler ohne Auswirkung auf die Freigabe.

Diese Ergebnisse und die Durchsicht durch das SIZ ergeben zwar einige Unschönheiten, die in Summe aber nur dazu führen, das System als Expertensystem einzustufen, d. h. für die Ergebnisse ist primär der bedienende Mitarbeiter verantwortlich. Auf Grund der erkennbaren Zusammenhänge im Ergebnis geht das SIZ trotz dieser Unschönheiten davon aus, dass das System insgesamt beherrschbar ist.

5.3.2 Vollständige Qualitätssicherung

Gefordert sind umfassende Tests durch den Hersteller. Umfassend bedeutet aus Sicht des SIZ: a) alle Zusagen, b) alle Positivtests und c) alle Negativtests.

Eine Überprüfung der zugesagten Eigenschaften hat der Hersteller in diversen Testprotokollen belegt [147].

Mit den geforderten Positivtests soll nachgewiesen werden, dass die IT-Anwendung ihre Kernfunktionalität tatsächlich erbringen kann. LORA wird von diversen Organisationen eingesetzt und auch die Prüfung erfolgt bereits zum widerholten Mal. Ein grundsätzlicher Funktionsnachweis muss damit für die Installation beim Betreiber als belegt angesehen werden.

Mit den geforderten Negativtests soll sichergestellt werden, dass die IT-Anwendung auch die zu erwartenden Störungen wie z. B. Fehleingaben und technische Ausfälle übersteht. Hierzu sind zwar einige wenige Tests dokumentiert, aber sowohl die Testergebnisse als auch die weiteren vorliegenden Informationen bestätigen, dass diese Störungen nur zum Teil abgefangen werden. Auch wenn dies für den Betrieb störend ist, so sind keine Störungen erkennbar, die einen Einsatz vollständig verhindern. Vom Einsatz dieser Software durch ungeübte Mitarbeiter ist trotzdem abzuraten.

5.3.3 Lasttest

Für LORA Speed ist ein Lasttest mit 33048 Aufträgen in der Datenbank dokumentiert [147, 3410, 14.2 Testanweisung] der eine Behandlung mit ca. 60 Sekunden dokumentiert.

5.4 Bereitstellung und Identifikation des Liefergegenstandes sowie seiner Quellen

5.4.1 Versionsverwaltung und Identifikation

Hinsichtlich der Versionierung eines ausgelieferten Produktes muss darauf hingewiesen werden, dass einem Institut auch eine Vorlagenanpassung ermöglicht wurde. **Für die Übermittlung der nach Releasewechseln ggf. geänderten Vorlagen an die beauftragten Gutachter ist allein das einsetzende Institut verantwortlich**.

Sämtliche Lieferbestandteile müssen als zusammengehörig identifizierbar sein[IDW PS 880, Tz5[9]], [IDW PS 880, Tz28]. Auf den primären produktspezifischen Dokumenten ist die Versionsnummer 2.4 bereits auf dem Deckblatt erkennbar. In den mit der Anwendung erstellten Beispielgutachten [129] ist die Versionsnummer der erstellenden Software nicht mehr auf Anhieb erkennbar. Ein potenzieller Verweis ergibt sich aus der Auftragsnummer und dem

[9] (IDW PS 880, Tz5) *Zu Beginn einer Prüfung von Softwareprodukten auf die Einhaltung von Ordnungsmäßigkeitsanforderungen und fachlichen Anforderungen ist eine Bestandsaufnahme des Prüfungsobjektes (Anwendungssoftware) und der Testumgebung (Hardwarekonfiguration, eingesetzte Betriebssystemkomponenten, ggf. Netzwerksoftware und Datenbankanwendungen) vorzunehmen. Voraussetzung hierfür ist das Vorliegen geeigneter Dokumentationsunterlagen.*



Kürzel (z. B.: 7LMPG), mit dem ein Dokument einem konkreten Erstellungsprozess zugeordnet werden kann.

5.4.1.1 Produktbeschreibung, Pflichtenheft oder Releasenotes

Die Produktbeschreibung der LORA Sparkassenedition [153] enthält widersprüchliche Versionsangaben. Das Deckblatt spricht bereits im April 2013 vom November 2013, während die Folgeseite die nachvollziehbare Angabe „Stand: März 2013“ trägt. Hier gilt damit die Versionsangabe auf dieser Folgeseite.

5.4.1.2 Systemdokumentation, Programmdokumentation, Softwaredesigndokumente

Für Herstellerinterne Dokumente wurde während der Prüfung festgestellt, dass hier nicht immer alle Dokumente eine Versionsnummer tragen und auch freizugebende Dokumente nicht immer formal freigegeben werden. Bei einem Vor-Ort-Termin in Erfurt in 2007 stellte sich das Designer- und Entwicklerteam aber als sehr überschaubar dar, so dass hieraus durch das SIZ neben dem rein formalen Problem keine weiteren Probleme benennbar sind und daher auch keine Auswirkungen auf den Freigabeprozess erkennbar sind.

5.4.1.3 Anwenderhandbuch und Hilfestellungen

Das Produkt LORA wird in seiner spezifischen Ausgestaltung durch verschiedene Handbücher beschrieben. Einige dieser Handbücher tragen zwar die Produktversionsnummer, nicht aber eine weitergehende Identifizierung. Da der Bereitstellungsprozess Pilotkunden und ggf. weitere Vorablieferungen berücksichtigt bei denen potenziell auch Veränderungen an Handbüchern erforderlich werden können ohne die Produktversionsnummer hoch zu zählen, ist damit nicht sichergestellt, dass alle Kunden mit einem nur die Produktversion referenzierenden Handbuch auch tatsächlich den gleichen Handbuchinhalt vorliegen haben. Prüfungsrelevante Aussagen finden sich im Literaturverzeichnis des Prüfberichtes (Abschnitt 3), zu diesem Zweck wird dort zu allen bereitgestellten Dokumenten neben deren Bezeichnung immer auch Dateidatum und Größe angegeben.

6 Detailbewertung aus Sicht der Benutzer bzw. Fachbereiche

6.1 Sicherstellung der Vollständigkeit von fachlichen Anforderungen

Schutzmechanismen vor ernsthaften Folgen auch bei Fehleingaben müssen transparent sein [2, 1.1.4.2], [3], [IDW PS 880, Tz15]. Das Benutzerhandbuch beschreibt die automatischen Kontrollen (Plausibilitätsprüfungen, siehe Abschnitt *5.2.2.2 Integration in den Geschäftsprozess*). Es macht aber auch darauf aufmerksam, dass durch das einsetzende Institut weitere manuelle Kontrollen erforderlich sind, z. B.:

- Für jedes Formular im Gutachtenteil gibt es eine Druckvorschau. In der Druckvorschau werden die auf diesem Formular eingegebenen Abschnitte in Word geöffnet und können dort kontrolliert werden[109, 4.6.12.1 Druckvorschau].
- Entsprechende Änderungen an den Stammdaten und den Berechtigungen für die Benutzer von LORA sind kompetenzgerecht durch die Organisation zu kontrollieren und zu dokumentieren[109, 4.3.5 Stammdaten Benutzer].

Die BelWertV stellt Anforderungen an die Prüfung von Gutachten, die zwar durch die IT-Anwendung unterstützt werden, fachlich aber durch entsprechendes Personal durchgeführt werden müssen.



6.2 Fachliche Berücksichtigung von gesetzlichen oder normativen Vorgaben

Die Produktbeschreibung [153, Zusammenfassung] liefert folgende Aussage: „*Die Bewertungssystematik wurde von Spezialisten der HypZert, RICS, BVS, großen Bewertungsgesellschaften, der Landes- und Pfandbriefbanken sowie der Sparkassen entwickelt, ist BAFin-konform und erfüllt alle gesetzlichen Vorgaben in der Wertermittlung wie WertV und BelWertV, BauGB und PfandBG. Mit LORA sind Sie damit in Bezug auf Konformität und Rechtssicherheit immer auf dem neuesten Stand. Zukünftig veränderte Forderungen werden im Zuge der Wartungs- und Pflegevereinbarung umgesetzt*“. Zur geprüften Umsetzung siehe die folgenden Abschnitte.

6.2.1 BauGB

Die Produktbeschreibung [153, Zusammenfassung] liefert folgende Aussage: „*Die Bewertungssystematik wurde von Spezialisten der HypZert, RICS, BVS, großen Bewertungsgesellschaften, der Landes- und Pfandbriefbanken sowie der Sparkassen entwickelt, ist BAFin-konform und erfüllt alle gesetzlichen Vorgaben in der Wertermittlung wie … BauGB … . Mit LORA sind Sie damit in Bezug auf Konformität und Rechtssicherheit immer auf dem neuesten Stand. Zukünftig veränderte Forderungen werden im Zuge der Wartungs- und Pflegevereinbarung umgesetzt*“.

6.2.2 BGB

Das Sicherheitshandbuch [152, 3.5 Externe Gutachter] legt dar, dass **Beauftragungen externer Gutachter** nicht **durch** *LORA* erfolgen, sondern **separate Vertragsabschlüsse (Beauftragungen)** erforderlich sind.

In der Anwendung werden potenziell externe Gutachter hinterlegt. [BGB, §241 Abs.2] in Verbindung mit [BGB, §311 Abs.2] definieren eine Geheimhaltungspflicht der mit Gutachtern existierenden Verträge. Der Zugriff auf die Anwendung selbst ist geschützt (siehe andere Abschnitte des Prüfberichtes), der Zugriff durch legitimierte Personen umfasst aber auch den Zugriff auf die Bezeichnungen der Gutachter. Hier ist auf die entsprechende Geheimhaltungsverpflichtung hinzuweisen.

Die ähnlich zu betrachtende Geheimhaltung von Mietverträgen, die nach Handbuch [153, Mietvertragsdatenbank] ebenfalls hinterlegbar sind, muss das einsetzende Institut entscheiden. Eine juristitische Prüfung dieses Sachverhaltes ist im SIZ nicht möglich und in den Produktunterlagen nicht dokumentiert. Verantwortungen sieht hier das SIZ aber weniger beim einsetzenden Finanzinstitut als vielmehr beim Vermieter, insofern bleibt dieser Konflikt für die Freigabe ohne weitere Folgen, siehe auch Abschnitt *6.2.3 BDSG*.

Zum Vertragswesen und der auf den WebSeiten des Herstellers vorhandenen Handelsplattform sind auch die Ausführungen im Abschnitt *4.2 Verwendung von Researchdaten* zu beachten.

6.2.3 BDSG

Für die Erhebung von personenbezogenen Daten muss eine Erlaubnis vorliegen [BDSG, §4]. Hierauf weist die Produktbeschreibung der Anwendung nicht hin. **Da inhaltlich nicht nur Name und Anschrift sondern auch genaue Beschreibungen der Immobilie und damit persönlicher Werte erfasst werden, muss durch das einsetzende Institut geklärt werden, ob die seitens Kunden erteilten Erlaubnisse zur Speicherung und potenziell auch der Weitergabe seiner Daten auch diese potenziellen Gutachteninhalte umfassen und es muss mit dem Datenschutzbeauftragten sichergestellt werden, das die für die Gutachten gespeicherten Daten auch im Verfahrensverzeichnis abgebildet sind**.

Inwieweit die nach Handbuch [153, Mietvertragsdatenbank] mögliche **Hinterlegung von** Mietvertragsdaten aus Sicht der **personenbezogenen Daten über Mieter zulässig ist,**



muss der DSB des einsetzenden Institutes entscheiden, das SIZ kann hier fachlich keine Erlaubnistatbestände erkennen, die aber ggf. vorhanden sein könnten.

Die Weitergabe von Personendaten, Eigentumsverhältnissen und anderen Daten zum Immobilieneigentum einer Person **an externe Gutachter unterliegen §11 BDSG und führen dazu, dass das einsetzende Institut für den Datenschutz bei dem externen Gutachter verantwortlich ist**, näheres siehe Abschnitt *8 Detailbewertung bei ganz oder teilweise ausgelagertem Betrieb*.

Personendaten, die nicht auf Grund von mit dieser Person bestehender Verträge erhoben werden (Interessentendaten), unterliegen zusätzlich zu ggf. relevanten Archivierungsfristen auch sogenannten Löschfristen, müssen also nach Ablauf bestimmter Fristen auch wieder gelöscht oder zumindest unlesbar gemacht werden [BDSG, §20], [COBIT4.0, DS11.4]. In der Anwendung LORA könnten potenziell auch Daten von Personen oder deren Eigentumsverhältnisse erfasst sein, mit denen kein Vertragsverhältnis existiert. Diese Daten müssten manuell innerhalb festzulegender Fristen entfernt werden. Da die Zulässigkeit der Speicherung allein schon entsprechende vorvertragliche Informationen zur Speicherung zwingend vorschreibt [BGB, § 491a Abs. 1] geht das SIZ davon aus, dass Institutsmitarbeiter erst einen entsprechenden Rahmenvertrag mit dem Institutskunden abschließen, bevor darüber hinaus gehende Daten erfasst werden.

6.2.4 BetrVG

Wenn Mitarbeiter bezogene Daten verarbeitet werden, darf darüber keine Kontrolle der Mitarbeiter möglich sein. LORA enthält zwar Hinweise auf letzte Bearbeiter und Protokolle zentraler Arbeitsschritte, die Vergabe von Bewertungsaufträgen ist aber nach Auffassung des SIZ eine so selten durchgeführte Tätigkeit, dass darüber keine Kontrolle eines Mitarbeiters abgeleitet werden kann.

6.2.5 GPSG

Für technische Arbeitsmittel sind Warnhinweise an den Stellen erforderlich, die zu andernfalls zu Schäden führen könnten. Diese Hinweise finden sich neben dem vorliegenden Prüfbericht auch in folgenden Handbüchern: der Produktbeschreibung [103, Plausibilisierung] und vor allem den Sicherheitshinweisen [152].

Es besteht grundsätzlich das Risiko, dass **Warnhinweise nicht im Gutachten** auftauchen. Als Fehlerquellen kommen hierbei primär die im Einzelfall verwendeten Vorlagen in Betracht, die aber **in der Verantwortung des einsetzenden Instituts** liegen, obwohl in den Produktunterlagen auf dieses Risiko nicht hingewiesen wird.

6.2.6 HGB

6.2.6.1 Handelsbriefe [HGB, §37a]

Die Kommunikation mit Geschäftspartnern (sogenannte Handelsbriefe) unterliegt einzuhaltenden gesetzlichen Regeln z. B. [GewO, §15b], [HGB, §37a], [GmbHG, §35a], [AktG, §80], gleichgültig ob diese über Briefpost oder elektronisch ausgetauscht wird. Die LORA-Anwendungen unterstützen den Anwender bei der Übermittlung von Daten an externe Gutachter. **Sowohl die eigentliche Auftragsvergabe als auch die erforderliche Archivierung der Handelsbriefe sind manuell durch den LORA-Anwender sicher zu stellen und werden durch die IT-Anwendung <u>nicht</u> geleistet**.

---

[10] Geräte- und Produktsicherheitsgesetz



Auch das Betriebshandbuch [122, 5.2 Datensicherung und Archivierung] spricht korrekt nur die Datensicherung an, Archivierungsmaßnahmen verbleiben damit in der Organisation des Betreibers.

An dieser Aussage ändert auch das Versprechen im Sicherheitshandbuch [152, 2.3.3 Archivierung und Backup] nichts, wenn dort ein nicht vorliegender *Nachweis einer gesetzeskonformen Archivierung* angesprochen wird.

6.2.6.2 Aufbewahrungspflichten [HGB, §257]

Archivfunktionen sind bei LORA organisatorisch zu leisten, den Sparkassen steht zur Archivierung eine Archivierungssoftware des Verbandsrechenzentrums zur Verfügung.

6.2.6.3 Vorlegung von Unterlagen auf Bild- und Datenträgern [HGB, §261]

Archivfunktionen sind bei LORA organisatorisch zu leisten, den Sparkassen steht zur Archivierung eine Archivierungssoftware des Verbandsrechenzentrums zur Verfügung.

6.2.7 PfandBG

Die Produktbeschreibung [153, Zusammenfassung] liefert folgende Aussage: „*Die Bewertungssystematik wurde von Spezialisten der HypZert, RICS, BVS, großen Bewertungsgesellschaften, der Landes- und Pfandbriefbanken sowie der Sparkassen entwickelt, ist BAFin-konform und erfüllt alle gesetzlichen Vorgaben in der Wertermittlung wie … PfandBG. Mit LORA sind Sie damit in Bezug auf Konformität und Rechtssicherheit immer auf dem neuesten Stand. Zukünftig veränderte Forderungen werden im Zuge der Wartungs- und Pflegevereinbarung umgesetzt*“.

6.2.8 UrhG

Bei der potenziellen Verwendung urheberrechtsgeschützter Vorlagen oder Anlagen ist ein Schutz vor Gesetzesverstößen erforderlich. Die LORA-Handbücher [153, Fotoverwaltung] und [153, Einbindung von Abbildungen] benennen die Möglichkeit zur Einbindung potenziell geschützter Objekte in die LORA-SparkassenEdition und LoraSpeed [103, Fotoverwaltung]. Dieser Schutz muss organisatorisch geleistet werden.

6.2.9 Verbraucherkreditrichtlinie

Zur IT-Anwendung LORA gehört ein optionaler Zugang zur Handelsplattform des Herstellers [151] mit der Möglichkeit, kostenpflichtige Bestellungen abzugeben.

Diese Funktionalität ist nach Abschnitt *1.2.2 Produktbeschreibung und -abgrenzung* aus dem Freigabeumfang ausgeklammert und damit durch den vorliegenden Prüfbericht <u>nicht</u> freigegeben.

Sofern diese Funktionalität erforderlich sein sein sollte, ist eine ausreichende Umsetzung <u>u. a.</u> folgender Themen nachzuweisen:

- [BGB, §126a Elektronische Form]
- [BGB, §145**ff**]
- [BGB, §312g Pflichten im elektronischen Geschäftsverkehr]
  Das dem SIZ bereitgestellte Dokument zur LORA-Handelsplattform [151] geht von abweichenden Rahmenbedingungen aus.
- [BGB,§360 Widerrufs- und Rückgabebelehrung]
- [BGB,§497 Verzug des Darlehensnehmers]



- [BGB,§510 Ratenlieferungsverträge]
- [BGBEG, Artikel 246, §1 Informationspflichten bei Fernabsatzverträgen]
- [BGBEG, Artikel 246, §2 Weitere Informationspflichten bei Fernabsatzverträgen]
- [BGBEG, Artikel 246, §3 Informationspflichten bei Verträgen im elektronischen Geschäftsverkehr]
  Das dem SIZ bereitgestellte Dokument zur LORA-Handelsplattform [151] geht von abweichenden Rahmenbedingungen aus.

6.2.10 AO (Abgabenordnung und Aufbewahrungsfristen), GoBS und Verarbeitung buchungsrelevanter Geschäftstransaktionen

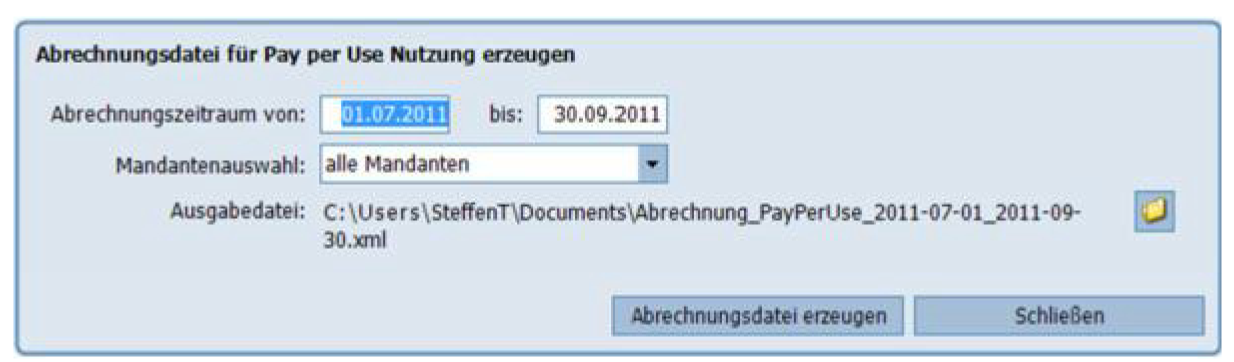
Der Hersteller erklärt hierzu:

> *LORA bietet den Kunden Unterstützung bei der Übertragung der Auftragsdaten in das jeweilige Buchungssystem. Der Kunde kann selbst die Druckvorlagen für die Buchungsausdrucke bearbeiten oder die Bearbeitung durch Dritte durchführen lassen. Eine automatisierte Übermittlung ist derzeit nicht vorgesehen. Die Übertragung ist nur über analoge Medien (Papierausdruck) möglich. Das System LORA stellt kein Buchungssystem oder System zur Rechnungslegung dar. Es können Vorlagen für das jeweilige Buchungssystem des Auftraggebers erzeugt werden. Inhalte, Form, Autorisierung und Archivierung obliegen allein dem Auftraggeber.*

Die Aussagen gelten auch hinsichtlich der mit LORA potenziell möglichen **Honorarberechnung** und dem in der Produktbeschreibung genannten **Rechnungsdruck** [153, Druck Auftrag, Rechnung und Laufzettel], **die**se **Funktionen sind** damit im Ergebnis der hier dokumentierten Prüfung als **unzulässig** zu betrachten.

LORA beliefert auch OSPlus mit Daten. Zu diesen Daten gehört nach Dokumentation des Herstellers [155] auch der sogenannte Beleihungswert, der im Rahmen einer bilanziellen Rücklage verwendet werden könnte. Nach Darstellung des OSPlus-Handbuches zum „Beleihungswert“, Zitat siehe Abschnitt *9.1 GLOSSAR*, geht der Prüfer hier von einem nicht rechnungslegungsrelevanten Wert aus.

Die Funktionsgruppe PayPerUse [141], die sich hinter folgender Maske verbirgt, ist separat zu betrachten:



[141, Abbildung 1: Vorhandener PayPerUse-Dialog in LORA]

- Für die diesen Daten zugrundeliegenden Nutzungen von Researchdaten und anderen separat beauftragten Geschäftsvorfällen gelten die Aussagen aus Abschnitt *4.2 Verwendung von Researchdaten*.
- Das oben im Kasten seitens Hersteller formulierte dargestellte Verbot einer Nutzung kann seitens SIZ nicht aufgehoben werden.



- Für diese Teilfunktion liegt mit [141] eine als „Verfahrensbeschreibung nach GoBS“ interpretierbare Beschreibung vor, bei der der Prüfer auf Grund spezieller Inhalte jedoch davon ausgegen muss, dass dieses Dokument einem anwendenden Institut nicht zur Verfügung gestellt würde und daher formal keine Einhaltung der GoBS vorliegen würde.

Das Sicherheitshandbuch [152, 2.1.2 Bestandteile der Software] beschreibt, dass '*alle Dateien im Ordner »print« - Druckvorlagen und Steuerdateien*' für die Mitarbeiter änderbar sein sollen. Eine solche Änderbarkeit schließt die Nutzung im Rahmen der Erstellung steuerrelevanter Ergebnisse aus.

6.2.11 BelWertV

Die Produktbeschreibung [153, Zusammenfassung] liefert folgende Aussage: „*Die Bewertungssystematik wurde von Spezialisten der HypZert, RICS, BVS, großen Bewertungsgesellschaften, der Landes- und Pfandbriefbanken sowie der Sparkassen entwickelt, ist BAFin-konform und erfüllt alle gesetzlichen Vorgaben in der Wertermittlung wie … BelWertV, …. Mit LORA sind Sie damit in Bezug auf Konformität und Rechtssicherheit immer auf dem neuesten Stand. Zukünftig veränderte Forderungen werden im Zuge der Wartungs- und Pflegevereinbarung umgesetzt*“.

Das Benutzerhandbuch zu LORA Sparkassenedition [109, 3.6 Plausibilisierung, Stichprobenüberprüfung] verweist auf §24 der BelWertV, dort ist eine *hinreichend große Zahl repräsentativer Stichproben* gefordert. **Da in der Anwendung die Prozentzahl einer Stichprobenziehung einzugeben ist und nicht die statistisch relevanten Parameter muss darauf hingewiesen werden, dass bereits die Prozentzahl mathematisch (Stochastik, Statistik) korrekt ermittelt werden muss**. Ähnlich verhalten sich die anderen Handbücher.

Eine weitere Überprüfung anderer Vorgaben der BelWertV hält das SIZ nicht für erforderlich, da die zu Vorversionen vorgelegten Nutzertreffen-Protokolle und Einzelanforderungen einschließlich der Testprotokolle eine intensive Beschäftigung mit der BelWertV aufzeigen, z.B. [145, R05, 1.2.2.4. Plausibilisierung].

Die Konkretisierung der BaFin zum Beleihungswert im Erbbaurecht [BAFIN-RS 13-2009] wurde in einem Konzept [142] berücksichtigt.

6.2.12 WertV

Die Produktbeschreibung [153, Zusammenfassung] liefert folgende Aussage: „*Die Bewertungssystematik wurde von Spezialisten der HypZert, RICS, BVS, großen Bewertungsgesellschaften, der Landes- und Pfandbriefbanken sowie der Sparkassen entwickelt, ist BAFin-konform und erfüllt alle gesetzlichen Vorgaben in der Wertermittlung wie WertV …. Mit LORA sind Sie damit in Bezug auf Konformität und Rechtssicherheit immer auf dem neuesten Stand. Zukünftig veränderte Forderungen werden im Zuge der Wartungs- und Pflegevereinbarung umgesetzt*“.

6.2.13 SolvV

Das Konzept zur Terminverfolgung benennt die Umsetzung der SolvV [144, 4.4 Offene Fragen]. Seitens SIZ können hier keine weiteren Informationen geliefert werden.



6.2.14 weitere Stellungnahmen und Verlautbarungen des Fachausschuss OPDV

6.2.14.1 Stellungnahme Nr. 1/1997 Besondere Ordnungsmäßigkeitsanforderungen bei elektronischer Archivierung/Aktenführung

LORA erfüllt gesetzliche und normative Archivierungsvorgaben nicht. Beim Einsatz in Sparkassen stellt dies nur ein organisatorisches Problem dar, da Sparkassen über das Verbandsrechenzentrum IT-Anwendungen zur Archivierung nutzen können und daher organisatorisch für ausreichend rechtssichere Archivierungen sorgen können.

Neben allgemeinen und in den Abschnitten *6.2.6 HGB* und *6.2.10 AO (Abgabenordnung und Aufbewahrungsfristen), GoBS und Verarbeitung buchungsrelevanter Geschäftstransaktionen* behandelten Themen werden Konkretisierungen benannt.

Die Stellungnahme [OPDV1-1997, 6. Dokumentation und Prüfbarkeit] weist auf spezifische Maßnahmen im IKS hin:

- Administration des Systems (Vorgaben und Nachweise),
- Kompetenzen und Berechtigungen, einschließlich Leseberechtigung für Prüfungszwecke (Festlegungen und Nachweise),
- Behandlung der Datenträger (Anweisungen und Nachweise),
- Datensicherung und -auslagerung (Regelungen und Nachweise),
- System-, Netzwerk- und Dateienmanagement (Vorgaben und Nachweise),
- Behandlung der Dokumente (Klassifizierung, Aufbewahrung/Vernichtung),
- Vorgaben für das Scanning (Handhabung, Funktionen und Kompetenzen),
- Vorgaben für die nachträgliche Bearbeitung gespeicherter Dokumente,
- manuelle Schnittstellen zu Datenübermittlungs- und sonstigen DV-Verfahren,
- Protokollierung der maschinellen und manuellen Abläufe,
- Qualitätsanforderungen und -kontrollen einschl. Nachweise (betriebsindividuell, z.B. in Abhängigkeit von Archivierungsverfahren und Dokumentenarten festlegen),
- Vorgaben für Retrievals und sonstige Auswertungen (z.B. Kompetenzen),
- Loggings zu Retrievals (mit Möglichkeit einer maschinellen Auswertung je nach Sensibilität der Dokumenteninhalte festlegen).

6.2.15 Standards des Institut der Wirtschaftsprüfer in Deutschland e.V. (IDW)

6.2.15.1 IDW RS FAIT 3, IDW Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung beim Einsatz elektronischer Archivierungsverfahren[11]

LORA erfüllt gesetzliche und normative Archivierungsvorgaben nicht. Beim Einsatz in Sparkassen stellt dies nur ein organisatorisches Problem dar, da Sparkassen über das Verbandsrechenzentrum IT-Anwendungen zur Archivierung nutzen können und daher organisatorisch für ausreichend rechtssichere Archivierungen sorgen können.

[11] Stand: 11.07.2006



Die folgende Tabelle stellt ersatzweise Themen des Rundschreibens (RS) dar und

- unterscheidet zwischen Programmfreigabe und Einsatzfreigabe, mithin zwischen Systemeigenschaft und organisatorisch durch das Institut zu leistenden Themen. **Für die Anwendung *LORA* wären** bei Bedarf **beide Gruppen organisatorisch sicherzustellen**.

Tz[12]	P[13]	E[14]	Hinweis
1-3	-	-	
4	-	X	**Das Institut muss Kenntnis über die Aufbewahrungspflichtigen Unterlagen haben**, dies könnten z. B. sein: Buchungsbelege, Handelsbücher und Handelsbriefe in elektronischer Form, physische Dokumente in Papierform (z. B. eingehende Handelsbriefe oder manuell erstellte Buchungsallongen und Belege), Verfahrens- und Anwenderdokumentationen, Dokumentation des IT-Kontrollsystems sowie sonstige zum Verständnis der Buchführung notwendige Unterlagen.
5-8	-	-	
9	X	X	Die Vernichtung der archivierten Dokumente ist zu regeln und umzusetzen.
10-14	-	-	
15	X 	 X	[HGB,§257], siehe Abschnitt 6.2.6.2 Aufbewahrungspflichten [HGB, §257] und [HGB,§261], siehe Abschnitt 6.2.6.3 Vorlegung von Unterlagen auf Bild- und Datenträgern [HGB, §261] sind einzuhalten
16-17	-	-	
18	X	(X)	Das BDSG ist einzuhalten, siehe Abschnitt 6.2.3 BDSG.
19		X	Das Steuergeheimnis ist zu wahren[AO,§30].
20-26	-	-	
27		X	Wenn das Scannen zur Betragsermittlung durchzuführender Transaktionen verwendet wird („frühes Archivieren“) gilt folgende Beispielgeschäftsprozessvorgabe:

[12] Die Tz-Nummern verweisen direkt auf die Nummerierung des Rundschreibens.

[13] Programmfreigaberelevant heißt in diesem Bericht behandelt.

[14] Einsatzfreigaberelevant heißt im Rahmen organisatorischer Maßnahmen durch das Institut zu leisten.

Tz[12]	P[13]	E[14]	Hinweis
			Eingang des Dokuments → Vorbereitung des Dokuments zum Scannen → Scannen des Dokuments am Scan-Client und Zuordnung der Dokumenten-ID → Kontrolle des Image auf Vollständigkeit und Richtigkeit (→ zurück zu Scannen) → Freigabe des Image → Weiterleitung des Image zur Erfassung der Buchungs-informationen → Erfassen der Buchungs-informationen im ERP-System → Buchungsfreigabe → (Automatische) Verknüpfung ERP-Ordnungskriterium und Dokumenten-ID im ERP-System → Ablage des Image auf Archiv-Server und Indexbildung → Kontrolle der Verknüpfung auf Vollständigkeit und Richtigkeit (→ zurück zur Verknüpfung) → Freigabe der Originaldokumente zur Vernichtung → ggf. Vernichtung des Originaldokuments
28-29	-	-	
30		X	Der Einsatz von Scannverfahren erfolgt − analog dem Archivierungsprozess „spätes Archivieren“ bei eingehenden Handelsbriefen − zur eindeutigen Identifikation und Zuordnung des Geschäftsvorfalls • entweder durch eine automatische Verknüpfung des gesamten Images mit dem Geschäftsvorfall mittels eines auf dem Ausdruck angebrachten Barcodes oder • durch eine manuelle Zuordnung des gescannten Images zu dem entsprechenden Geschäftsvorfall.
31-37	X	X	Behandlung von ▪ rechtlichen (siehe Abschnitt *2.4 Einhaltung gesetzlicher oder bankaufsichtsrechtlicher Vorschriften*), ▪ technischen (siehe Abschnitt *2.3 Auswirkungen auf das Sicherheitsniveau*) und ▪ organisatorischen Risiken (siehe kompletten Abschnitt *2 Details zur Risikoklassifizierung*). Beachtet werden muss: ▪ Unzureichende organisatorische Festlegungen und Verfahrensanweisungen können die Nachvollziehbarkeit und Anwendbarkeit der Archivierungsverfahren gefährden. ▪ Mangelhafte Zugriffskontrollen innerhalb des Archivierungssystems ermöglichen die missbräuchliche oder unautorisierte Einsichtnahme der archivierten Dokumente und Daten.

Tz[12]	P[13]	E[14]	Hinweis
			▪ Durch Veränderungen, Manipulationen oder Löschung der archivierten Daten und Dokumente wird deren Integrität, Authentizität oder Verfügbarkeit verletzt. Mangelnde Integrität und Authentizität haben zur Folge, dass Geschäftsvorfälle inhaltlich nicht zutreffend abgebildet werden. ▪ Fehler bei der Indexierung von archivierten Dokumenten führen dazu, dass diese im Archivierungssystem nicht mehr auffindbar sind. Integritätsverletzungen haben zur Folge, dass aufzeichnungspflichtige Geschäftsvorfälle nicht oder nur unvollständig archiviert werden. ▪ Fehlende Regelungen von Verantwortlichkeiten für das Archivierungsverfahren sowie eine unzureichende Integration des Archivierungssystems können zum Verlust von archivierten Daten und Dokumenten führen. ▪ Durch Änderungen des IT-Systems können Inkompatibilitäten entstehen, welche die Lesbarkeit der archivierten Unterlagen über den gesamten Aufbewahrungszeitraum gefährden. Mangelhafte Migrationskonzepte bzw. Fehler bei der Datenmigration können dazu führen, dass archivierte Dokumente aus Altsystemen (Altdaten) nicht in ein neu eingeführtes Archivierungssystem übernommen werden können. Ebenso können beim Wechsel des Rechnungslegungssystems aufgrund von Schnittstellenproblemen Inkompatibilitäten auftreten, die einen Zugriff auf die archivierten Dokumente und Daten verhindern. ▪ Unzureichende Migrationskonzepte können z.B. bei der Nutzung von Technologiesprüngen bei Speichermedien die Beweiskraft der Buchführung gefährden. ▪ Die rechtlichen, technischen und organisatorischen Risiken muss der Buchführungspflichtige über den gesamten Aufbewahrungszeitraum berücksichtigen.
38-48	X	(X)	Der Schutz der Vertraulichkeit ist durch die Autorisierungsmechanismen gegeben, die im Abschnitt *7.4.1 Identifikation / Authentisierung (K101)* näher beschrieben sind. Hierbei wird auch die Autorisierung behandelt. Zum Schutz der Integrität und Authentizität ist die Vollständigkeit der bearbeiteten Dokumente im Archiv manuell zu prüfen. Dies ist im Abschnitt *6.4 Internes Kontrollsystem (IKS) der Sparkasse* näher erläutert. Die Verfügbarkeit und Verbindlichkeit setzt eine ausreichend originalgetreue Verfügbarkeit während der Anwendungslaufzeit, beschrieben im Abschnitt *7.4.7 Hochverfügbarkeit (K348)*, und nach Anwendungseinsatz voraus, beschrieben im Abschnitt *6.2.6.3 Vorlegung von Unterlagen auf Bild- und Datenträgern [HGB, §261]*. Die Themen des HGB, Vollständigkeit, Richtigkeit, Zeitgerechtheit, Nachvollziehbarkeit und Unveränderlichkeit sind im Abschnitt *6.2.6 HGB* bzw. dessen Unterabschnitten sowie im Abschnitt *6.2.10 AO (Abgabenordnung und Aufbewahrungsfristen), GoBS und Verarbeitung buchungsrelevanter Geschäftstransaktionen* beschrieben.
49		X	Einsatzrisiken und deren Reduktion werden in den Abschnitten *2 Details*



Tz[12]	P[13]	E[14]	Hinweis
			zur Risikoklassifizierung und *4.1 Auflagen* behandelt.
50-51	X	X	Archivierungsprozesse und deren Ablauforganisation sind zu dokumentieren. Hinweise liefert insbesondere Abschnitt *5.2.3 Programm- bzw. Systemdokumentation*.
52-82	X	X	Die technischen Sicherungsmaßnahmen und entsprechende organisatorische Maßnahmen sind in den Abschnitten *4.1 Auflagen* und *7.4 Sicherstellung eines sicheren IT-Betriebes* benannt.
83-85	X	X	Überwachungsmaßnahmen sind in den Abschnitten *4.1 Auflagen* und *6.4 Internes Kontrollsystem (IKS) der Sparkasse* benannt.
86-88	X	X	Bei der Auslagerung relevante Aspekte sind in den Abschnitten *4.1 Auflagen*, *7.4.5* SLV Sicherheitsanforderungen (K307) und *8 Detailbewertung bei ganz oder teilweise ausgelagertem Betrieb* benannt.

6.2.16 Control Objectives for Information and related Technology (COBIT) der Information Systems Audit and Control Association (ISACA)

Die für eine einzelne IT-Anwendung nach COBIT zu untersuchenden Aspekte (Control Objetives) werden in anderen Abschnitten dieses Prüfberichtes behandelt. Eine erste Referenz gibt hier der Index unter COBIT, eine Detailgegenüberstellung befindet sich in folgender Tabelle.

Control Objective aus COBIT	Referenz auf Abschnitt des Prüfberichtes
PO1.1 IT Value Management / Management des Wertbeitrags der IT	5.1 Nachvollziehbares Projektmanagement
PO1.2 Business-IT Alignment / Ausrichtung Kerngeschäft und IT	5.4 Bereitstellung und Identifikation des Liefergegenstandes sowie seiner Quellen 5.4.1 Versionsverwaltung und Identifikation 5.4.1.1 Produktbeschreibung, Pflichtenheft oder Releasenotes
PO2.1 Information Architecture Model / Informationsarchitekturmodell	5.2 Fehlerfreie Herstellung der IT-Anwendung 5.2.2 Architektur und Schnittstellendesign, Geschäftsprozessmodellierung (GPM)
PO2.2 Enterprise Data Dictionary and Data Syntax Rules / Unternehmensweites Data Dictionary und Datensyntaxregeln	5.2 Fehlerfreie Herstellung der IT-Anwendung 5.2.2 Architektur und Schnittstellendesign, Geschäftsprozessmodellierung (GPM)
PO2.3 Data Classification Scheme / Datenklassifikationsschema	5.2 Fehlerfreie Herstellung der IT-Anwendung 5.2.2 Architektur und Schnittstellendesign, Geschäftsprozessmodellierung (GPM)

Control Objective aus COBIT	Referenz auf Abschnitt des Prüfberichtes
PO2.4 Integrity Management / Handhabung der Integrität	5.2 Fehlerfreie Herstellung der IT-Anwendung 5.2.2 Architektur und Schnittstellendesign, Geschäftsprozessmodellierung (GPM)
PO3.3 Monitoring of Future Trends and Regulations / Überwachung von zukünftigen Trends und Bestimmungen	5.1 Nachvollziehbares Projektmanagement
PO3.5 IT Architecture Board / IT Architekturgremium	5.2 Fehlerfreie Herstellung der IT-Anwendung 5.2.2 Architektur und Schnittstellendesign, Geschäftsprozessmodellierung (GPM)
PO4.6 Roles and Responsibilities (Rollen und Verantwortlichkeiten	7 Detailbewertung aus Sicht des Betreibers 7.4 Sicherstellung eines sicheren IT-Betriebes 7.4.1 Identifikation / Authentisierung (K101)
PO4.9 Data and System Ownership / Daten und Systemeignerschaft	5.2 Fehlerfreie Herstellung der IT-Anwendung 5.2.2 Architektur und Schnittstellendesign, Geschäftsprozessmodellierung (GPM)
PO4.11 Segregation of Duties / Funktionstrennung	5.2 Fehlerfreie Herstellung der IT-Anwendung 5.2.3 Programm- bzw. Systemdokumentation 6 Detailbewertung aus Sicht der Benutzer bzw. Fachbereiche 6.2 Fachliche Berücksichtigung von gesetzlichen oder normativen Vorgaben 6.2.3 BDSG 7 Detailbewertung aus Sicht des Betreibers 7.4 Sicherstellung eines sicheren IT-Betriebes 7.4.1 Identifikation / Authentisierung (K101)
PO5.5 Benefit Management / Nutzenmanagement	5.2 Fehlerfreie Herstellung der IT-Anwendung 5.2.2 Architektur und Schnittstellendesign, Geschäftsprozessmodellierung (GPM)
PO10.5 Project scope statement / Beschreibung des Projektumfangs	5.1 Nachvollziehbares Projektmanagement
PO10.7 Integrated Project Plan / Integrierter Projektplan	5.1 Nachvollziehbares Projektmanagement
PO10.8 Project Resources / Projekt-Ressourcen	5.1 Nachvollziehbares Projektmanagement



Control Objective aus COBIT	**Referenz auf Abschnitt des Prüfberichtes**
PO10.9 Project Risk Management / Projekt-Risikomanagement	5.1 Nachvollziehbares Projektmanagement
PO10.10 Project Quality Plan / Projekt-Qualitätsplan	5.3 Nachweis einer vollumfänglichen Qualitätssicherung
PO10.14 Project Closure / Projektabschluss	5.1 Nachvollziehbares Projektmanagement
AI1.4 Requirements and Feasibility Decision and Approval / Freigabe der Anforderungsdefinition und Machbarkeit	5.2 Fehlerfreie Herstellung der IT-Anwendung 5.2.1 Anforderungserfassung (AE)
AI2.1 High level Design / Grobdesign	5.2 Fehlerfreie Herstellung der IT-Anwendung 5.2.2 Architektur und Schnittstellendesign, Geschäftsprozessmodellierung (GPM)
AI2.2 Detailed Design / Detailliertes Design	5.2 Fehlerfreie Herstellung der IT-Anwendung 5.2.2 Architektur und Schnittstellendesign, Geschäftsprozessmodellierung (GPM)
AI2.3 Application Control and Auditability / Anwendungskontrollen und Nachvollziehbarkeit)	5.2 Fehlerfreie Herstellung der IT-Anwendung 5.2.2 Architektur und Schnittstellendesign, Geschäftsprozessmodellierung (GPM)
AI2.4 Application Security and Availability / Sicherheit und Verfügbarkeit der Anwendung	5.2 Fehlerfreie Herstellung der IT-Anwendung 5.2.2 Architektur und Schnittstellendesign, Geschäftsprozessmodellierung (GPM) 5.2.2.1 Schnittstellen und sicherer Datenaustausch
AI2.8 Software Quality Assurance / Software-Qualitätssicherung	5.3 Nachweis einer vollumfänglichen Qualitätssicherung
AI2.10 Application Software Maintenance / Wartung von Anwendungssoftware	5.1 Nachvollziehbares Projektmanagement
AI4.3 Knowledge Transfer to End Users / Transfer von Knowledge an den Endbenutzer	5.4 Bereitstellung und Identifikation des Liefergegenstandes sowie seiner Quellen 5.4.1 Versionsverwaltung und Identifikation 5.4.1.3 Anwenderhandbuch und Hilfestellungen
AI5.1 Procurement Control /Steuerung der Beschaffung	7 Detailbewertung aus Sicht des Betreibers 7.4 Sicherstellung eines sicheren IT-Betriebes 7.4.5 SLV Sicherheitsanforderungen (K307)



Control Objective aus COBIT	Referenz auf Abschnitt des Prüfberichtes
AI5.3 Supplier Selection / Lieferantenauswahl	7 Detailbewertung aus Sicht des Betreibers 7.4 Sicherstellung eines sicheren IT-Betriebes 7.4.5 SLV Sicherheitsanforderungen (K307)
AI5.5 Acquisition of Development Resources / Beschaffung von Entwicklungsressourcen	6 Detailbewertung aus Sicht der Benutzer bzw. Fachbereiche 6.2 Fachliche Berücksichtigung von gesetzlichen oder normativen Vorgaben
AI5.6 Acquisition of Infrastructure, Facilities and Related Services / Beschaffung von Infrastruktur, Einrichtungen und entsprechenden Diensten	7 Detailbewertung aus Sicht des Betreibers 7.4 Sicherstellung eines sicheren IT-Betriebes 7.4.5 SLV Sicherheitsanforderungen (K307)
AI7.1 Training /Schulung	5.4 Bereitstellung und Identifikation des Liefergegenstandes sowie seiner Quellen 5.4.1 Versionsverwaltung und Identifikation 5.4.1.3 Anwenderhandbuch und Hilfestellungen
DS5.3 Identity Management / Identitätsmanagement	7 Detailbewertung aus Sicht des Betreibers 7.4 Sicherstellung eines sicheren IT-Betriebes 7.4.1 Identifikation / Authentisierung (K101)
DS5.4 User Account Management / Management von Benutzerkonten	7 Detailbewertung aus Sicht des Betreibers 7.4 Sicherstellung eines sicheren IT-Betriebes 7.4.1 Identifikation / Authentisierung (K101)
DS5.7 Protection of Security Technology /Schutz von Sicherheitseinrichtungen	7 Detailbewertung aus Sicht des Betreibers 7.4 Sicherstellung eines sicheren IT-Betriebes 7.4.3 Key- Management (K108)
DS5.8 Cryptographic Key Management / Verwaltung kryptographischer Schlüssel	7 Detailbewertung aus Sicht des Betreibers 7.4 Sicherstellung eines sicheren IT-Betriebes 7.4.3 Key- Management (K108)
DS5.10 Network Security / Netzwerk-Sicherheit	7 Detailbewertung aus Sicht des Betreibers 7.4 Sicherstellung eines sicheren IT-Betriebes 7.4.2 Vertrauenswürdige Kanäle (K106)
DS5.11 Exchange of Sensitive Data / Austausch sensitiver Daten	7 Detailbewertung aus Sicht des Betreibers 7.4 Sicherstellung eines sicheren IT-Betriebes



Control Objective aus COBIT	Referenz auf Abschnitt des Prüfberichtes
DS11.4 Disposal / Entsorgung	7.2 Installation und Betriebsaufnahme

6.2.17 Mindestanforderungen an das Risikomanagement (MaRisk) der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)

[MARISK, AT7.2 Technisch-organisatorische Ausstattung] fordert Freigaben auf Anwendungsanpassungen. Das Handbuch [153, Anpassung Druckdateien (Word-Dot Dateien)] benennt die Möglichkeit, u. a. auch die Rechnungsstellung anzupassen ohne darauf hinzuweisen, dass entsprechende Anpassungen nach [MARISK, AT7.2 Technisch-organisatorische Ausstattung] einer neuen Freigabe bedürfen. Da eine Rechnungslegung entsprechend Abschnitt *6.2.10 AO (Abgabenordnung und Aufbewahrungsfristen), GoBS und Verarbeitung buchungsrelevanter Geschäftstransaktionen* unzulässig ist, bleibt diese Feststellung im Rahmen der hier dokumentierten Prüfung ohne weitere Folgen.

6.3 Korrekte Bedienung durch den Anwender

Bei einer IT-Anwendung ist zu berücksichtigen, dass Betriebsstörungen auftreten und behandelt werden müssen. Das Anwenderhandbuch beschreibt den Umgang mit potenziellen Fehlern [109, 4.9.9 Fehler im Programm] und auch wie die Kundenbetreuung [109, S.IV] durch den Hersteller erreichbar ist.

6.4 Internes Kontrollsystem (IKS) der Sparkasse

Dem einsetzenden Institut muss eine Kontrolle des Zugriffsschutzes möglich sein. Das Betriebshandbuch [149, 2.2 Verantwortlichkeiten und Zugriffsberechtigungslogik] liefert eine grobe Einordnung und das Benutzerhandbuch [109, 4.3.5.1 Stammdaten Interner Mitarbeiter] eine grobe Beschreibung der Berechtigungsmasken.

Die erforderlichen Eingabe- [2, 3.2] und Verarbeitungskontrollen [2, 3.3] sind in LORA immer durch eine manuelle Prüfung der erstellten Reports durchzuführen. Die Vorgehensweise sind in den entsprechenden Handbüchern beschrieben. **Es ist eine aus Institutssicht korrekte Kontrolle der erstellten Gutachten zu definieren und in LORA zu konfigurieren**, Details finden sich im Abschnitt *5.2.2.2 Integration in den Geschäftsprozess*.

7 Detailbewertung aus Sicht des Betreibers

7.1 Sicherstellung der Vollständigkeit von technischen Anforderungen

Die Produktbeschreibung [153, Webfähigkeit und Hosting] benennt die Lauffähigkeit unter Citrix.

7.2 Installation und Betriebsaufnahme

Nach einer Installation muss für den Betreiber erkennbar sein, ab wann die Installation und Erstkonfiguration des Systems als abgeschlossen gelten kann. Das Installationshandbuch [119, 5 Erster Start] benennt lediglich erste Maßnahmen. Weitere Detailinformationen werden dem Betreiber in einem speziellen zur Lizenz passenden „erste-Schritte“-Dokument geliefert [110] benannt. Das Sicherheitshandbuch [152, 2.1.7 Funktionstest] fasst die signifikanten Funktionstests zusammen.

Zum erforderlichen [HGB, §239 Abs. 3] Nachweis eines unveränderten Einsatzes ist eine ausreichende Transparenz über Änderungsberechtigungen an Dateien und Datenbanken

erforderlich. Diese Transparenz wird durch das Betriebshandbuch [149, 2.5 LORA Softwarekomponenten] hergestellt.

7.3 Betriebsbereitschaft in einer Sparkasse oder deren VRZ

7.3.1 Fremdkomponenten

7.3.1.1 Betriebssystem, Laufzeitumgebungen und andere Fremdkomponenten

Das Sicherheitshandbuch [152, 2.1.1 Erforderliche Software-Komponenten] weist darauf hin, dass weitere Softwarekomponenten beim Einsatz von LORA seitens Betreiber vorausgesetzt werden. Kosten und Sicherheitsupdates trägt damit das einsetzende Institut, die Liste umfasst allerdings neben der Datenbank nur Standardanwendungen von Microsoft.

Die Softwareüberlassung umfasst [106, 8 Schutzrechte Dritter] die Zusicherung seitens on-geo, „*den Kunden gegen alle Ansprüche verteidigen, die aus einer Verletzung des Urheberrechtes durch das vertragsgemäß genutzte Lizenzmaterial gegen den Kunden hergeleitet werden*“. Die Frage nach der korrekten Lizensierung mitgelieferter Module stellt sich damit für das einsetzende Institut nicht mehr.

7.3.2 Betrieb und Abrechnung

Sofern neben einer Einstiegslizenz und potenziellen Wartungskosten weitere Kosten im Betrieb auftreten, muss deren Höhe transparent werden [SITB, K359 (Leistungsverrechnung)], [HGrG, §6 Abs.3]. Hierzu liefert der Hersteller eine Preisliste [108]. Die hier relevanten Kosten beziehen sich entweder auf Hosting oder auf die Bereitstellung von Researchdaten zu Immobilien, beide Fälle sind durch den vorliegenden Prüfbericht <u>nicht</u> abgedeckt, deshalb erfolgt für diesen Fall keine Bewertung durch das SIZ.

Das SIZ weist darauf hin, dass neben den vom Hersteller genannten Kosten folgende weiteren Kosten anfallen können:

- LORA kann auf einem kostenpflichtigen Server abgelegt werden, dabei auf kostenpflichtige Dateiablagen und Datenbanken zugreifen und Datenübertragungskosten verursachen, die vom jeweiligen Preismodell der Provider abhängen.
- LORA kann auf die kostenpflichtige dynamische Schnittstelle der Finanz Informatik (FI) zugreifen.

7.4 Sicherstellung eines sicheren IT-Betriebes

7.4.1 Identifikation / Authentisierung (K101)

Die Authentisierung bei Archivfunktionen sind bei LORA organisatorisch zu leisten, den Sparkassen steht zur Archivierung eine Archivierungssoftware des Verbandsrechenzentrums zur Verfügung.

In einer Datenbank hinterlegte Daten sind bei Verwendung eines sogenannten technischen Users maximal so geschützt wie auch die außerhalb der Datenbank liegende Anmeldekennung dieses technischen Users. Auch wenn die OPDV-Stellungnahme 1/2003 die Verschlüsselung von Passworten ohne Rückrechenbarkeit vorsieht, so ist dieses Verhalten bei der Speicherung der Anmeldedaten des technischen Users nicht möglich. U. a. das Betriebshandbuch [149, 4.6.3 Beendigung des Betriebs] dokumentiert die Existenz eines solchen technischen Users in LORA. Das Sicherheitshandbuch [152, 2.1.4 Zugriffsschutz für Datenbank und Online-Dienste] legt dem Administrator entsprechende Schutzmaßnahmen auf.



7.4.2 Vertrauenswürdige Kanäle (K106)

Datenübertragungswege insbesondere bei Verwendung von E-Mail müssen entsprechend des Schutzbedarfs der übermittelten Daten ausreichend verschlüsselt sein [COBIT4.0, DS5.10], [COBIT4.0, DS5.11], [SITB, K106] , [SITB, K109], [GS-KAT, M2.119 (Regelung für den Einsatz von E-Mail)]. Gutachten mit einer detaillierten Beschreibung des Eigentums einer Person werden per E-Mail zwischen Gutachtern und deren Auftraggebern ausgetauscht. Der Hersteller stellt eine technische Beschreibung zur Verfügung aus der ein Datentransfer mit einer symmetrischen Rijndael-Verschlüsselung mit 128bit Verschlüsselung hervorgeht, die aktuell als ausreichend sicher einzustufen ist. Eine solche Bewertung kann sich aber in Zukunft ändern.

7.4.3 Key- Management (K108)

Schlüssel sind ausreichend vor unzulässiger Erzeugung, Änderung, Widerrufung, Zerstörung, Verteilung, Zertifizierung, Speicherung, Eingabe, Verwendung und Archivierung zu schützen [COBIT4.0, DS5.8], [SITB, K108]. Das Benutzerhandbuch [109, 4.4.4.13.1 Verschlüsselungscode] beschreibt die Existenz von Schlüsseln zum Datenaustausch mit Gutachtern. Hierbei hat auch der Administrator ein Zugriffsrecht auf diese Schlüssel, um sie mit dem Gutachter auszutauschen. Selbst eine unzulässige Weitergabe der Schlüssel und eine passend fehlerhafte Konfiguration der E-Mail Verbindung bedingt, dass auch auf der Partnerseite eine LORA-Installation vorliegt. Nur die Kenntnis des Schlüssels und des dazugehörigen Verfahrens erlauben einem Empfänger nur, die fertig gestellten Gutachten, nicht aber deren Aufträge auszulesen. Der Versand der fertigen Gutachten wird aber nicht im einsetzenden Institut, sondern beim Gutachter final konfiguriert. Ein signifikantes Restrisiko für das einsetzende Institut kann derzeit durch das SIZ nicht identifiziert werden.

Das Sicherheitshandbuch [152, 2.1.4 Zugriffsschutz für Datenbank und Online-Dienste] beschreibt die Lesbarkeit der Accountdaten für Datenbankzugriff und Onlinezugriffe für Mitarbeiter. Als Lösung wird der optionale Einsatz eines Verschlüsselungstools empfohlen. **Die Verschlüsselung der der Accountdaten für Datenbankzugriff und Onlinezugriffe sieht das SIZ** nicht als optional sondern **als verpflichtend an**. Das Testprotokoll [147,, R01, S.40] bestätigt die potenzielle Möglichkeit der unverschlüsselten Passwortablage.

7.4.4 Berechtigungskonzept (K115)

Das Berechtigungssystem muss dokumentiert sein [SITB, K115]. Das Betriebshandbuch [149, 2.2 Verantwortlichkeiten und Zugriffsberechtigungslogik] liefert eine grobe Einordnung und das Benutzerhandbuch [109, 4.3.5.1 Stammdaten Interner Mitarbeiter] eine grobe Beschreibung der Berechtigungsmasken.

Bei Mehrmandantensystemen sind die Daten der Mandanten zu trennen [SITB, L.03], [IDW PS 880, Tz12]. Es ist weder erkennbar, dass Gutachter, die mehrere Kunden und damit Auftraggeber für Gutachten jeden ihrer Kunden als einzelnen Mandanten ansehen und deren Daten mehr als technisch notwendig trennen, noch sind in LORA Funktionen beschrieben, die eine entsprechende Mandantentrennung zulassen. Die Problematik betrifft primär einen externen Gutachter und nur in zweiter Linie auch ein einsetzendes Institut, insofern bleibt es im Rahmen der Prüfung bei dieser Feststellung.

7.4.5 SLV Sicherheitsanforderungen (K307)

Fragen zu diesem Abschnitt würden relevant, wenn Archivierungen im Rahmen der Auslagerung an z.B. den Hersteller zu betrachten wären. Da diese Funktion aber durch den vorliegenden Prüfbericht nicht legitimiert wird, findet keine weitere Betrachtung statt.

---

[15] http://en.wikipedia.org/wiki/Two-factor_authentication#Biometrics



7.4.6 Datensicherung (K318)

Eine vollständige Datensicherung muss möglich sein. Das Betriebshandbuch spricht diese Tätigkeit an mehreren Stellen [149, 4.1 Periodische Tätigkeiten], [149, 5.2 Datensicherung und Archivierung] an und beschreibt immer alle bekannten zu sichernden Objekttypen.

Der mögliche Zeitpunkt einer Datensicherung muss transparent sein. Hierzu machen die Produktunterlagen keine Aussagen, da es sich aber um eine typische Client-Anwendung handelt, ist der Sicherungszeitpunkt entsprechend der üblichen Sicherungszeiten zu wählen.

7.4.7 Hochverfügbarkeit (K348)

Fragen zu diesem Abschnitt würden relevant, wenn Funktionen im Rahmen der Auslagerung an z.B. den Hersteller zu betrachten wären. Da diese Funktion aber durch den vorliegenden Prüfbericht nicht legitimiert wird, findet keine weitere Betrachtung statt.

7.5 Technische Berücksichtigung von weiteren gesetzlichen oder normativen Vorgaben

7.5.1 GPSG

Auch der Betreiber muss ausreichend auf Gefahrensituationen hingewiesen werden, sofern daraus Schäden entstehen können. Das Löschen des letzten administrativ berechtigten Users in der Datenbank ist möglich. Danach ist die weitere Administration einem Betreiber nicht mehr möglich und kann ggf. erst nach kostenpflichtigem Vor-Ort-Einsatz des Herstellers wieder hergestellt werden. Auf diese Gefahr macht das Betriebshandbuch <u>nicht</u> aufmerksam. Ein Hinweis auf diese Gefahrenquelle findet sich aber im Berechtigungskonzept sowie ohne signifikante Hervorhebung im Benutzerhandbuch [109, S.90 „Aussperren aus der Rechteverwaltung“]. Da Administratoren bei der Löschung administrativer Zugänge i. d. R. auch ohne Dokumentation sehr vorsichtig umgehen, hält das SIZ diesen Hinweis hier für ausreichend.

8 Detailbewertung bei ganz oder teilweise ausgelagertem Betrieb

Potenziell relevant werden hier folgende Aspekte:

- Die Vergabe von Aufträgen zur Bewertung an externe Gutachter wird auch im Sicherheitshandbuch [152, 3.5 Externe Gutachter] entsprechend angesprochen. **Für die Einhaltung des BDSG bei der Auftragsverarbeitung durch externe Gutachter ist das einsetzende Institut verantwortlich**. Inhaltlich liegt diese Beziehung <u>nicht</u> im Prüfungsumfang der hier dokumentierten Prüfung. Hinweise könnten die folgenden Abschnitte des Prüfberichts hier trotzdem liefern.
- Supportleistungen des Herstellers oder auch das Hosting der IT-Anwendung durch den Hersteller, stellt wegen personenbezogener Daten eine BDSG-relevante Auftragsdatenverarbeitung oder Funktionsübertragung dar. **Das einsetzende Institut ist für die Einhaltung des BDSG in dieser Konstellation verantwortlich**. Der Hersteller erklärte gegenüber dem SIZ, dass bislang kein verwertbares Ergebnis eines Datenschutzaudits vorliegt, Details siehe Abschnitt *8.1.2 §11 BDSG, §§241,311 BGB - Datenschutz*.
- In wie weit die Verwendung von Research-Daten als Auslagerung einzustufen ist oder ob hier auch Vorgaben aus dem BDSG relevant werden, liegt außerhalb der hier dokumentierten Prüfung.

Der vorliegende Prüfbericht wird das Vorliegen oder Nicht-Vorliegen eines rechtlich relevanten ausgelagerten Betriebes nicht juristisch verbindlich beantworten können. Hierzu müssten über die technischen Gegebenheiten, die Bestandteil des Prüfberichts sind auch reale Geschäftsprozesse des einsetzenden Institutes mit betrachtet werden als auch die nicht vorhandene juristische Verbindlichkeit des Prüfberichts angenommen werden. Dieser Prüfbericht liefert daher die folgenden Informationen lediglich aus dem Blickwinkel der späteren Betrachtungserfordernisse von technischen Gegebenheiten bei einer im Einsatz theoretisch möglichen Annahme des Vorliegens eines ausgelagerten Betriebs.

Zur risikoorientierten Steuerung und Überwachung der Auslagerung von IT-Services gibt es die OPDV Stellungnahme Nr. 1/2009 [49].

An die Auslagerung von Geschäftsprozessen oder deren Teilen bestehen gesetzliche und normative Anforderungen, die einzuhalten sind. Aktuell [39] sind dies folgende Vorgaben:

- §25a Abs. 2 KWG, §33 WpHG
- §16 InvG
- §14 Abs. 3 GwG
- §§269-293, 322, 337 Solvabilitätsverordnung
- Mindestanforderungen an das Risikomanagement 5/2007
- Rundschreiben 17/2005 Finanzierung aus einer Hand

8.1 Gesetzliche und normative Vorgaben

8.1.1 HGB

Im Falle der Verwendung von Researchdaten [153, Integration Research-Daten] oder beim Hosting [153, Webfähigkeit und Hosting] ist zu klären, in wie weit die von Drittfirmen bereitgestellten Daten ebenfalls unter das BDSG fallen. Zumindest ist nach BDSG das Verhältnis zu diesen Drittfirmen zu benennen.

8.1.2 §11 BDSG, §§241,311 BGB - Datenschutz

Unabhängig von der Feststellung, ob eine rechtlich relevante Auslagerung vorliegt oder nicht, stellt die Tatsache, dass der Betrieb der Anwendung nicht durch das Institut selbst sondern durch ein Rechenzentrum betrieben wird, eine nach BDSG relevante Auftragsdatenverarbeitung dar, dies gilt auch für Supportleistungen durch den Hersteller, sofern dieser dabei Zugang zu den daten erhält.

Die Produktbeschreibung [153, Webfähigkeit und Hosting] und [153, Integration Research-Daten] sowie das FI-Rundschreiben Nr. 206/2009 benennen das potenzielle Vorliegen einer entsprechenden Auftragsverarbeitung.

Der dem SIZ vorgelegte Pflegevertrag [104] ist nicht BDSG-konform, auch die Hinweise [105] stellen keine Konformität her.

Final zu bewerten ist nicht ein potenziell existierender Mustervertrag, sondern der tatsächlich zwischen einsetzendem Institut und Betreiber vereinbarte Vertrag, insofern haben die folgenden Aussagen nur vorläufigen Charakter. **Das einsetzende Institut muss prüfen, ob alle Belange ausreichend erfüllt sind**.

gesetzliche Vorgabe an den Vertragsinhalt nach BDSG §11 Abs. 2 (BDSG-Novelle II: In Kraft getreten am 1. September 2009 zum Thema Auftragsdatenverarbeitung)	**Hinweis auf Behandlung im Mustervertrag**

gesetzliche Vorgabe an den Vertragsinhalt nach BDSG §11 Abs. 2 (BDSG-Novelle II: In Kraft getreten am 1. September 2009 zum Thema Auftragsdatenverarbeitung)	**Hinweis auf Behandlung im Mustervertrag**
Gegenstand und Dauer des Auftrages	
Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, deren Art und der konkrete Kreis der davon Betroffenen	
die nach §9 BDSG zu treffenden technischen und organisatorischen Schutzmaßnahmen (Mussvorgabe!)	
Grundvorgaben zur Berichtigung, Löschung und Sperrung von Daten	
nach §11 Abs. 4 BDSG bestehende Pflichten des Auftragnehmers, insbesondere diejenigen von ihm vorzunehmenden Kontrollen	
eventuelle Erlaubnis gegenüber dem Auftragnehmer zur Einschaltung von Subunternehmern	
Kontrollrechte des Auftraggebers und die sich daraus ergebenden Duldungspflichten des Auftragnehmers (Mussvorgabe für Auftraggeber zur Durchführung solcher Kontrollen)	
mitteilungspflichtige Verstöße des Auftragnehmers oder bei ihm beschäftigter Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen im Auftrag getroffene Vereinbarungen	
Rahmen und Umfang von Weisungsbefugnissen, die zugunsten des Auftraggebers gegenüber dem Auftragnehmer bestehen	
Rückgaberegelungen bezüglich überlassener Datenträger und Vorgaben zur Löschung von beim Auftragnehmer gespeicherten Daten nach Auftragsbeendigung	

9 ANLAGEN

9.1 GLOSSAR

BEGRIFF ⇱	**DEFINITION**
Abnahmetest	Der Abnahmetest dient dem Ziel, zu zeigen, dass das Vertrauen in das System für den produktiven Einsatz gerechtfertigt ist
Angemessen [ISO/IEC 9126]	Entsprechend [IDW EPS 300, Tz8] stellt in der hier vorliegenden Dokumentation dieser Begriff *die „Angemessenheit“ der Prüfungsnachweise einen qualitativen Maßstab für die eingeholten Prüfungsnachweise, deren Verlässlichkeit und Relevanz für die Prüfung einer Aussage in der Rechnungslegung dar*. Siehe auch „ausreichend“.
Ausreichend	Entsprechend [IDW EPS 300, Tz8] stellt in der hier vorliegenden Dokumentation dieser Begriff keine Schulnote dar sondern beschreibt lediglich einen quantitativen Maßstab,



BEGRIFF ↸	DEFINITION
	siehe auch „angemessen“.
Beleihungswert	[FI-Handbuch - OSPlus KFp (8-7/11) - Beleihungswert C 15.4.1]: „*Im Prozessschritt "Beleihungswert" wird Ihnen der in der Beratung vorläufig ermittelte Beleihungswert angezeigt, den Sie weiter modifizieren können (C 15.4.1.1 OSPlus-Kredit Finanzierungen (portalrein)*[16]*). Als weitere Informationen erhalten Sie die Angaben zum Objekt und die ausgewählte Finanzierungsvariante. …* o *In dem Prozessschritt "Beleihungswert" werden Ihnen ausschließlich die Werte der vorläufigen Wertermittlung aus der Beratung angezeigt. Wenn Sie den Beleihungswert modifizieren möchten, können Sie dies über das Vereinfachte Abschlagsverfahren tun (C 15.4.1.1 OSPlus-Kredit Finanzierungen (portalrein)). Klicken Sie dazu die Schaltfläche [Beleihungswert] an.* o *Alternativ kann dieser Prozessschritt ohne weitere Aktion mit [Weiter] verlassen werden. Dann bekommen Sie die in der Abbildung angezeigte Hinweismeldung angezeigt. Wenn Sie die Hinweismeldung mit [Weiter] bestätigen, verlassen Sie diesen Prozessschritt. Der Beleihungswert kann ggf. im Rahmen der Bearbeitung von VVS modifiziert werden.*“
Qualität	DIN ISO 8402 (Entwurf März 1992): "*Die Gesamtheit von Merkmalen einer Einheit (entity in der engl. Fassung) bezüglich ihrer Eignung, festgelegte und vorausgesetzte Erfordernisse zu erfüllen*." DIN 55350 (Teil 11) : "*Qualität ist die Gesamtheit von Eigenschaften und Merkmalen eines Produkts oder einer Tätigkeit, die sich auf deren Eignung zur Erfüllung gegebener Erfordernisse bezieht.*" Qualität ist kein absoluter Wert, sondern muss immer relativ zu gegebenen Erfordernissen gesehen werden. Qualitätsbewertungen beinhalten also immer einen Vergleich zwischen Qualitätsvorgaben, die aus den gegebenen Erfordernissen abgeleitet werden (Soll-Werte) und den tatsächlich erreichten Ausprägungen der Merkmale (Ist-Werte). Qualität ist ein Maß für die Erfüllung von Anforderungen.
Schutzbedarf	Eine spezifische Voraussetzung der IT-Sicherheit eines bestimmten Systems, also eine notwendige Bedingung zur Sicherung der Integrität und Verfügbarkeit des Systems sowie der Informationsvertraulichkeit innerhalb des Systems. Schutzbedürfnisse sind sehr konkret formulierte Erfordernisse der IT-Sicherheit eines Systems. Sie identifizieren seine Verwundbarkeiten, indem sie das schutzbedürftige Objekt (Subsystem), seinen konkreten Schutzbedarf und (vorzugsweise) die Konsequenzen mangelnden Schutzes nennen. Sie antworten auf die Fragestellung "Welches konkrete Objekt braucht welchen Schutz zur Vermeidung welcher Gefahr?" oder, salopper formuliert, "Was muss im einzelnen verhindert

---

[16] http://v000aplsis01.intern/grundangebot/vonfi/handbuecher/parsys/ospkpv-e.nsf/834559db1fef73dd41256a23003dbac9/c63f1e0088e0cff5c12577670045f720?OpenDocument



BEGRIFF ↖	DEFINITION
	werden?"
Sicherheit	Die Kombination aus Vertrauenswürdigkeit, Integrität und Verfügbarkeit.
SITB	[SITB] Der „Sichere IT-Betrieb des SIZ" beschreibt Sicherheit entsprechend aller für Finanzinstitute in Deutschland geltenden Regeln und bietet auch eine Zertifizierung nach SITB an. Viele Sparkassen haben ihr Sicherheitsmanagement entsprechend SITB zertifizieren lassen.



10 INDEX


INFORMATIKZENTRUM
DER SPARKASSEN-
ORGANISATION GMBH

11 Unterschrift

Bonn, Dienstag, 11. Juni 2013	Dipl. Inform. Bernhard König (Prüfer)	Dr. Thomas Stock (Qualitätssicherung des vorliegenden Prüfberichtes, siehe Änderungshistorie)